Zentyal 3.0 Official Documentation

Introduction to Zentyal

- Presentation
  - SMBs and ITC
  - Zentyal: Linux server for SMBs
- Installation
  - Zentyal installer
  - Initial configuration
  - Hardware requirements
- First steps with Zentyal
  - Administrative web interface of Zentyal
  - Network configuration with Zentyal
- Software updates
  - Management of Zentyal components
  - System Updates
  - Automatic updates
- Zentyal Remote Client
  - About Zentyal Remote
  - Registering Zentyal server to Zentyal Remote
  - Configuration backup in Zentyal Remote
  - Other services along with your registration

Zentyal Infrastructure

- Zentyal Infrastructure
- High-level Zentyal abstractions
  - Network objects
  - Network services
- Domain Name System (DNS)
  - DNS cache server configuration with Zentyal
  - Transparent DNS Proxy
  - DNS Forwarders
  - Configuration of an authoritative DNS server with Zentyal
- Time synchronization service (NTP)
  - Configuring an NTP server with Zentyal
- Network configuration service (DHCP)
  - DHCP server configuration with Zentyal
- Thin client service (LTSP)
  - Configuration of a thin client server with Zentyal
  - Download and run thin client
- Certification authority (CA)
  - Certification Authority configuration with Zentyal
- Virtual private network (VPN) service with OpenVPN
  - Configuration of a OpenVPN server with Zentyal
- Virtual private network (VPN) service with PPTP
  - Configuring a PPTP server in Zentyal
- Virtual Private Network (VPN) Service with IPsec
  - Configuring an IPsec tunnel in Zentyal
- Virtualization Manager
  - Creating virtual machines with Zentyal
  - Virtual machine maintenance

Zentyal Gateway

- Zentyal Gateway
- Firewall
  - Firewall configuration with Zentyal
- Routing
  - Configuring routing with Zentyal
- Quality of Service (QoS)

    - Quality of service configuration in Zentyal
- Network authentication service (RADIUS)
    - Configuring a RADIUS server with Zentyal
- HTTP Proxy Service
    - HTTP Proxy configuration in Zentyal
    - Access Rules
    - Filter profiles
    - Bandwidth Throttling
- Captive Portal
    - Configuring a captive portal with Zentyal
    - Exceptions
    - List of Users
    - Using the captive portal
- Intrusion Detection System (IDS)
    - Configuring an IDS with Zentyal
    - IDS Alerts

Zentyal Office

- Zentyal Office
- Directory Service (LDAP)
    - Configuration of an LDAP server with Zentyal
    - User's corner
- File sharing and authentication service
    - Configuring a file server with Zentyal
    - Configuring a Domain Controller with Zentyal
- File Transfer Protocol (FTP)
    - FTP server configuration with Zentyal
- Web publication service (HTTP)
    - Introduction to HTTP
    - HTTP server configuration with Zentyal
- Printers sharing service
    - Printer server configuration with Zentyal
- Backup
    - Zentyal configuration *Backup*

Zentyal Unified Communications

Zentyal Unified Communications

- Zentyal Unified Communications
- Electronic Mail Service (SMTP/POP3-IMAP4)
  - SMTP/POP3-IMAP4 server configuration with Zentyal
- Mail filter
  - Mail filter schema in Zentyal
- Webmail service
  - Configuring a webmail in Zentyal
- Groupware service
  - Configuration of a groupware server (Zarafa) with Zentyal
  - Zarafa basic use cases
- Instant Messaging Service (Jabber/XMPP)
  - Configuring a Jabber/XMPP server with Zentyal
- Voice over IP service
  - *VoIP* server configuration with Zentyal
  - Using Zentyal VoIP features

Zentyal Maintenance

- Zentyal Maintenance
- Logs
  - Zentyal log queries
  - Configuration of Zentyal logs
  - Log Audit for Zentyal administrators
- Events and alerts
  - Events and alerts configuration in Zentyal
- Uninterruptible power supply
  - UPS Configuration with Zentyal
- Monitoring
  - Monitoring in Zentyal
  - Metrics
  - Bandwidth Monitoring
  - Alerts
- Automatic Maintenance with Zentyal Remote
  - Zentyal Remote
  - Troubleshooting
  - Maintenance

- Maintenance
  - Remote management and inventory
  - Free trials

Advanced Zentyal Management

- Importing configuration data
- Advanced Service Customisation
- Development environment of new modules
- Release policy
  - Zentyal Release Cycle
  - Support policy
- Bug management policy
  - Patches and security updates
- Technical support
  - Community support
  - Commercial support

Copyright 2004-2012 Zentyal S.L.

Presentation

SMBs and ITC

About **99% of companies in the world** are small and medium businesses (SMBs). They generate more than half of the global GPD. SMBs constantly look for ways to **reduce costs** and **increase productivity**, especially in times of crisis like the one we are currently facing. However, they often operate under **very limited budgets** and **limited workforces**. These circumstances make it extremely challenging to offer suitable solutions that bring important benefits, at the same time keeping investments and operational costs within budget.

Technology vendors have traditionally shown little interest in developing solutions that adapt to the needs of SMBs. In general, enterprise solutions available on the market have been developed for large corporations and therefore their implementation requires considerable investments of time and resources, as well as a high level of expertise.

In the server market, this has meant that until now SMBs have had few solutions to choose from and in addition, the available solutions have usually been over-sized. Considering the real needs of SMBs - too complex to manage and with high licensing costs.

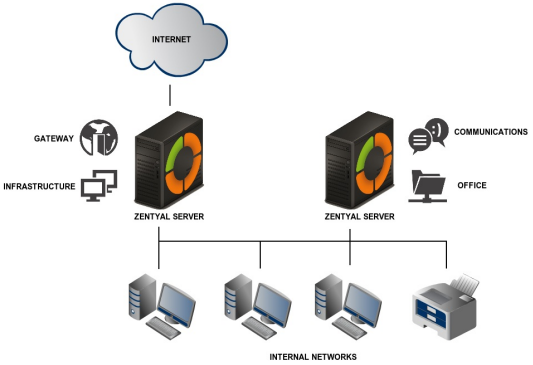
In this context it seems reasonable to consider **Linux** as a more attractive SMB server alternative, since technically it has shown very high **quality** and functionality, and the acquisition **price** is unbeatable. However, the presence of *Linux* in SMB environments is symbolic and the growth is relatively small. How is this possible?

We believe that the reason why this happens is simple: to adapt an enterprise level server to an SMB environment, the components must be well integrated and easy to administer. Similarly, the ICT service providers that work for SMBs also need server solutions, that require low deployment and maintenance time to stay competitive. Traditional Linux server distributions don't offer these characteristics.

Zentyal: Linux server for SMBs

Zentyal [1] was developed with the aim of bringing **Linux** closer to SMBs and to allow them to make the most of its potential as a corporate server. It is the open source alternative to Microsoft network infrastructure products aimed at SMBs (Windows Small Business Server, Windows Server, Microsoft Exchange, Microsoft Forefront, ...)

Server, Windows Server, Microsoft Exchange, Microsoft Forefront...) and it is based on the popular *Ubuntu* distribution. Zentyal allows IT professionals to manage all network services such as Internet access, network security, resource sharing, network infrastructure or communications in an easy way via **one single platform**.



Example of a Zentyal deployment performing different roles

During its development, the focus has been the usability. Zentyal offers a n **intuitive interface**, that includes the most frequently needed features. Although there are other, some more complex, methods used to carry out all kinds of advanced configurations. Zentyal incorporates independent applications into fully integrated functions **automating most tasks**. This is designed to save systems management time.

Given that 42% of security issues and 80% of service outages in companies are due to human error in the configuration and administration of these systems [2], Zentyal is a solution that is not only **easier** to manage, but also more **secure and reliable**. To sum up, besides offering significant savings, Zentyal improves security and availability of network services within the companies.

The Zentyal development began in 2004 under the name of *eBox Platform* and it has grown to become a widely used and highly recognised solution, The platform integrates **over 30** open source systems and network management tools into a single technology. Zentyal has been included in *Ubuntu* since 2007 and since 2012 the commercial editions are officially supported by Canonical - the company behind the development of Ubuntu - currently Zentyal is downloaded **over 1,000 times every day** and has an active community of thousands of members.

There are tens of thousands of active Zentyal installations, mainly in America and Europe, although its use is extended to virtually every country on earth. The US, Germany, Spain, Brazil and Russia are the countries with most installations. Zentyal is mainly used in SMBs, but **also in other environments** such as schools, governments, hospitals and even in prestigious institutions such as *NASA*.

Zentyal development is funded by Zentyal S.L. Zentyal is full-featured Linux server that can be used for free without technical support or

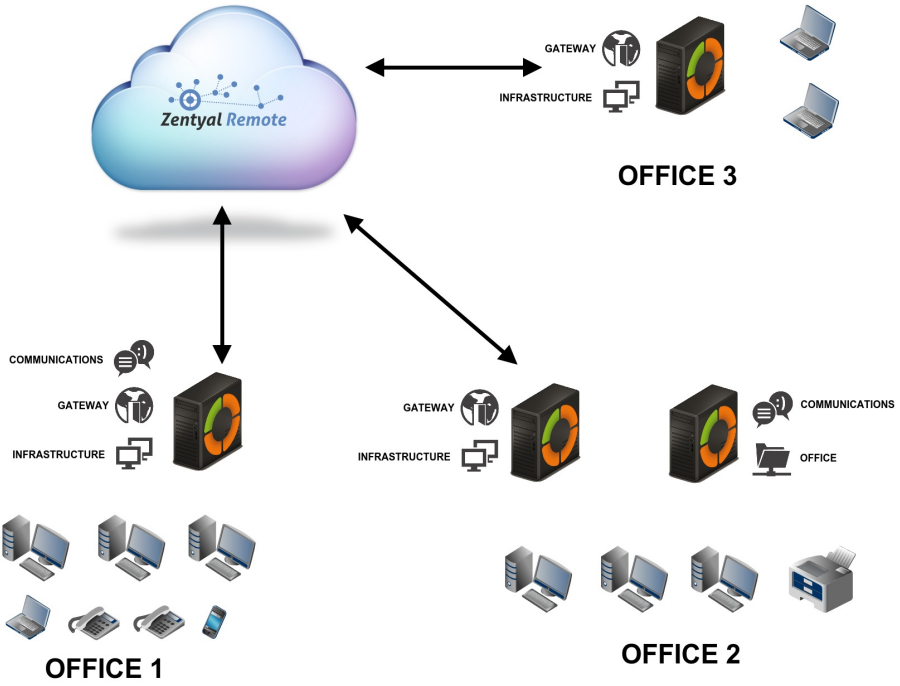
updates, or fully supported for a reasonable monthly fee. The commercial editions are aimed at two clearly different type of customers. On one hand **Small Business Edition** is aimed at small businesses with less than 25 users and with one single server or very simple IT infrastructure. On the other hand, **Enterprise Edition** is aimed at small and medium businesses with more than 25 users and more complex IT infrastructure.

The commercial editions come with the following services and tools:

- **Full technical support** by Zentyal Support Team
- **Official support guaranteed by Ubuntu/Canonical**
- **Software and security updates**
- **Remote monitoring and management platform** of servers and desktops
- **Disaster recovery**
- **Proxy HTTPS**
- **Multiple server administrators**

Zentyal S.L. also offers the following cloud-based services that can be integrated in the commercial editions of the Zentyal server or used independently:

- **Cloud-based email solution**
- **Cloud-based corporate file sharing solution**



In case that small and medium businesses want to count on support from a local IT provider to deploy a Zentyal-based system, they can contact Authorized Zentyal Partners. These partners are local IT support and service providers, consultants or managed service providers that offer consultancy, deployment, support and/or outsourcing of infrastructure and network services of their customers. To find the closest Zentyal Partner, or to learn how to become a partner, please visit the Partner section at zentyal.com [3].

Zentyal S.L. offers to the Authorized Zentyal Partners a series of tools and services that help at **reducing the maintenance costs** of IT infrastructure of their customers and offering managed services with high added value:

- **Support platform**
- **Remote monitoring and management platform** of servers and desktops
- **Training and certification of technical and sales staff**
- **Managed services portfolio**
- **Sales materials**
- **Lead generation program**
- **Discounts**

[1] http://www.zentyal.com/
[2] http://enise.inteco.es/enise2009/images/stories/Ponencias/T25/marcos%20polanco.pdf
[3] http://www.zentyal.com/partners/

This documentation describes the main technical features of Zentyal, helping you to understand the way you can configure different network services with Zentyal and **become productive** when managing SMB ICT infrastructure with Linux based systems.

The documentation is divided into six chapters plus some appendices. This first introductory chapters helps to understand the context of Zentyal as well as the installation process and walks you through the first steps required to use the system. The following four chapters introduce you to the four typical installation profiles: Zentyal as a network infrastructure server, as a server giving access to the Internet or *Gateway*, as an office server or as a communications server. This differentiation into four functional groups is only made to facilitate the most typical Zentyal deployments. It is also possible to deploy any combination of Zentyal server functionality.

Finally, the last chapter describes the tools and services available to **carry out and simplify the maintenance** of a Zentyal server, ensuring its smooth running, optimising its deployment, resolving incidents and recovering the system in case of a disaster.

Copyright 2004-2012 Zentyal S.L.

Installation

Generally speaking, Zentyal is meant to be installed exclusively on one (real or virtual) machine. However, this does not prevent you from installing other applications, that are not managed through the Zentyal interface. These applications must be manually installed and configured.

Zentyal runs on top of *Ubuntu* [1] server edition, always on LTS (*Long Term Support*) [2] versions. LTS has longer support periods: five years instead of three.

You can install Zentyal in two different ways:

- using the Zentyal installer (recommended option),
- using an existing *Ubuntu Server Edition* installation.

In the second case the official Zentyal repositories must be added and installation continued by installing the modules you are interested in [3].

However, in the first case the installation and deployment process is easier as all dependencies reside on a single CD or USB. Another benefit of using the CD or USB is to have a graphical environment that allows the use of a web interface from the server itself.

Ubuntu's official documentation includes a brief introduction to installing and configuring Zentyal [4].

[1] *Ubuntu* is a *Linux* distribution developed by *Canonical* and the community, focused on laptops, PCs and servers: http://www.ubuntu.com/.

[2] For a detailed description about the publication of *Ubuntu* versions it is recommended you consult the *Ubuntu* guide: https://wiki.ubuntu.com/Releases.

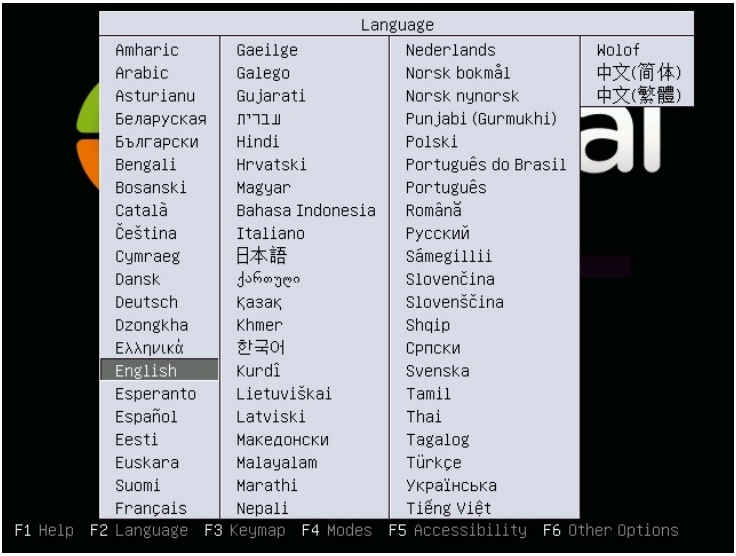
[3] For more information about installing from the repository please go to http://trac.zentyal.org/wiki/Document/Documentation/InstallationGuide.

[4] https://help.ubuntu.com/12.04/serverguide/zentyal.html

Zentyal installer

The Zentyal installer is based on the *Ubuntu Server* installer. Those already familiar with this installer will also find the installation process very similar.

To start with, you choose the installation language, in this example *English* is chosen.



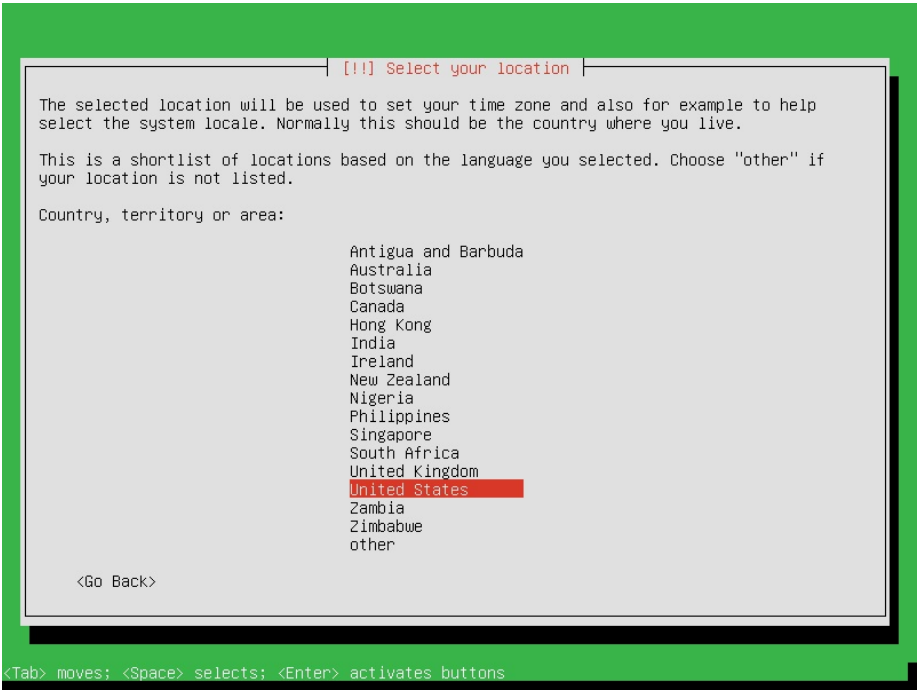
Selection of the language

You can install Zentyal by using the default mode which deletes all disk contents and creates the partitions required by Zentyal by using *LVM* [5] or you can choose the expert mode which allows customised partitioning. Most users should choose the default option unless they are installing on a server with RAID software or they want to create special partitioning according to specific requirements.

zentyal
Install Zentyal 3.0 (delete all disk)
Install Zentyal 3.0 (expert mode)
Check disc for defects
Test memory
Boot from first hard disk
Rescue a broken system
F1 Help F2 Language F3 Keymap F4 Modes F5 Accessibility F6 Other Options

Installer start

In the next step choose the language for your system interface. To set the language, you are asked for your country, in this example the *United States* is chosen.

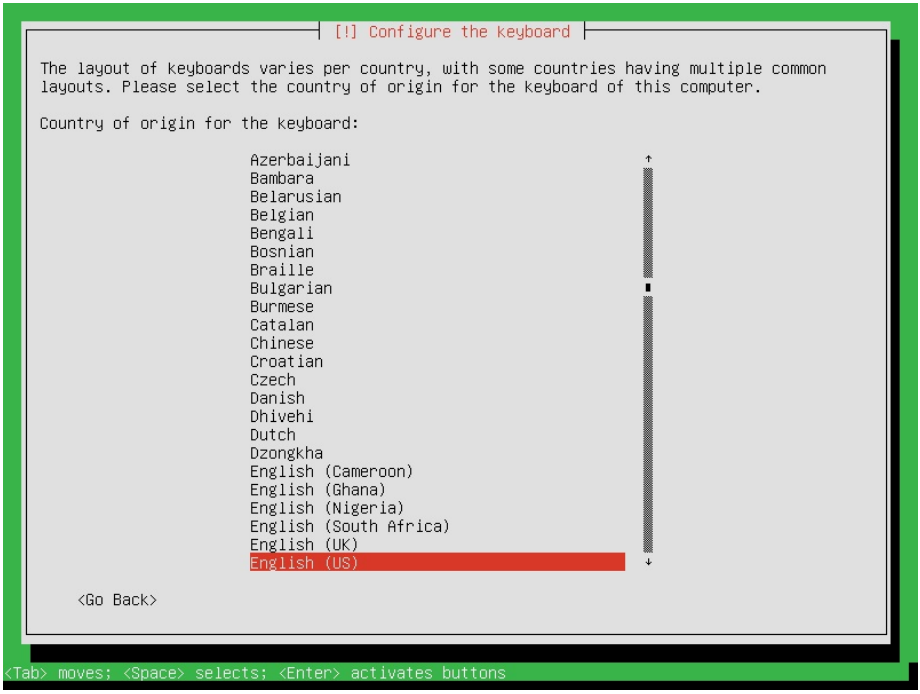


Geographical location

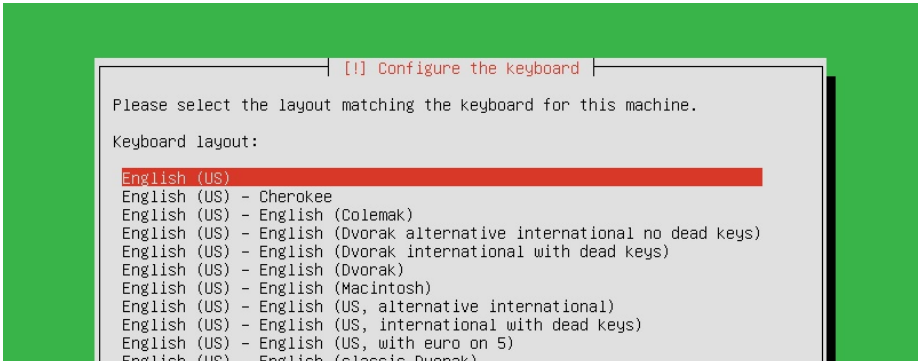
You can use automatic detection for setting the keyboard: a few questions are asked to ensure the model you are using is correct. Otherwise, you can select the model manually by choosing *No*.

[!] Configure the keyboard
You can try to have your keyboard layout detected by pressing a series of keys. If you do not want to do this, you will be able to select your keyboard layout from a list.
Detect keyboard layout?
<Go Back>
<Yes>
<No>

Keyboard configuration 1



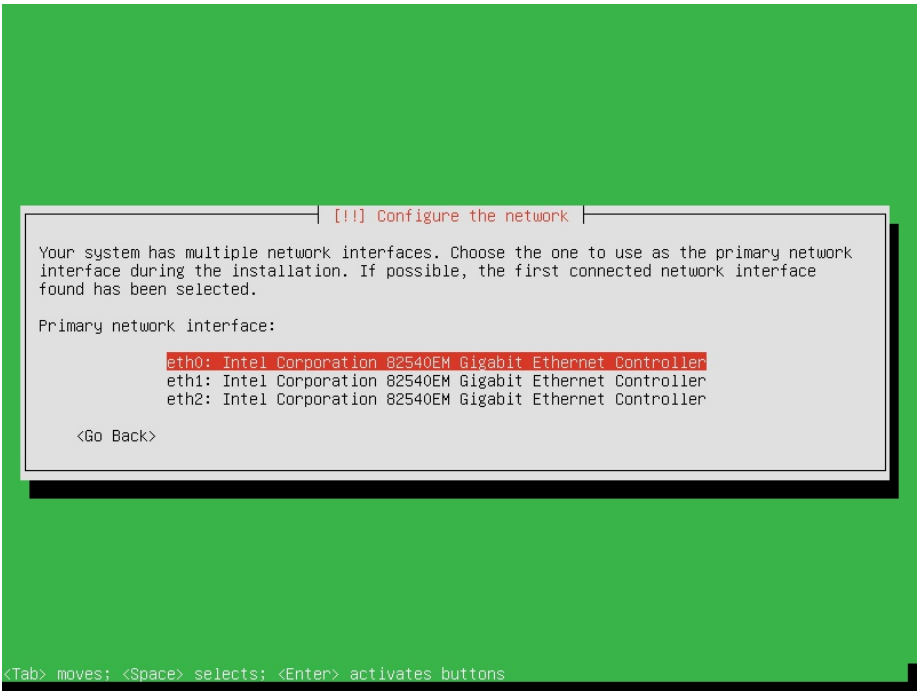
Keyboard configuration 2


[!] Configure the keyboard
Please select the layout matching the keyboard for this machine.
Keyboard layout:
English (US)
English (US) - Cherokee
English (US) - English (Colemak)
English (US) - English (Dvorak alternative international no dead keys)
English (US) - English (Dvorak international with dead keys)
English (US) - English (Dvorak)
English (US) - English (Macintosh)
English (US) - English (US, alternative international)
English (US) - English (US, international with dead keys)
English (US) - English (US, with euro on 5)

English (US) - English (classic Dvorak)
English (US) - English (international AltGr dead keys)
English (US) - English (layout toggle on multiply/divide key)
English (US) - English (left handed Dvorak)
English (US) - English (programmer Dvorak)
English (US) - English (right handed Dvorak)
English (US) - Russian (US, phonetic)
English (US) - Serbo-Croatian (US)
<Go Back>
<Tab> moves; <Space> selects; <Enter> activates buttons

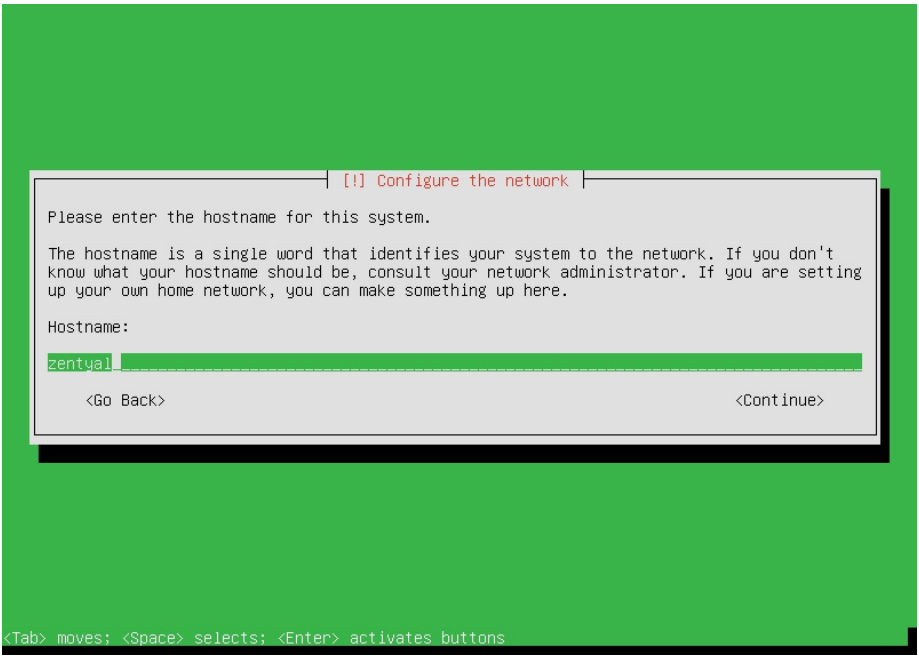
Keyboard configuration 3

If you have multiple network adapters, the installer will ask you for your primary one , the one that will be used to access the Internet during the installation. The installer will try to auto configure it using DHCP. If you only have one interface, you will not see this question


[!!] Configure the network
Your system has multiple network interfaces. Choose the one to use as the primary network interface during the installation. If possible, the first connected network interface found has been selected.
Primary network interface:
eth0: Intel Corporation 82540EM Gigabit Ethernet Controller
eth1: Intel Corporation 82540EM Gigabit Ethernet Controller
eth2: Intel Corporation 82540EM Gigabit Ethernet Controller
<Go Back>
<Tab> moves; <Space> selects; <Enter> activates buttons

Select primary network interface

Now choose a name for your server: this name is important for host identification within the network. The *DNS* service will automatically register this name. *Samba* will also use this domain name, as you will see later.


[!] Configure the network
Please enter the hostname for this system.
The hostname is a single word that identifies your system to the network. If you don't know what your hostname should be, consult your network administrator. If you are setting up your own home network, you can make something up here.
Hostname:
zentyal
<Go Back>
<Continue>
<Tab> moves; <Space> selects; <Enter> activates buttons

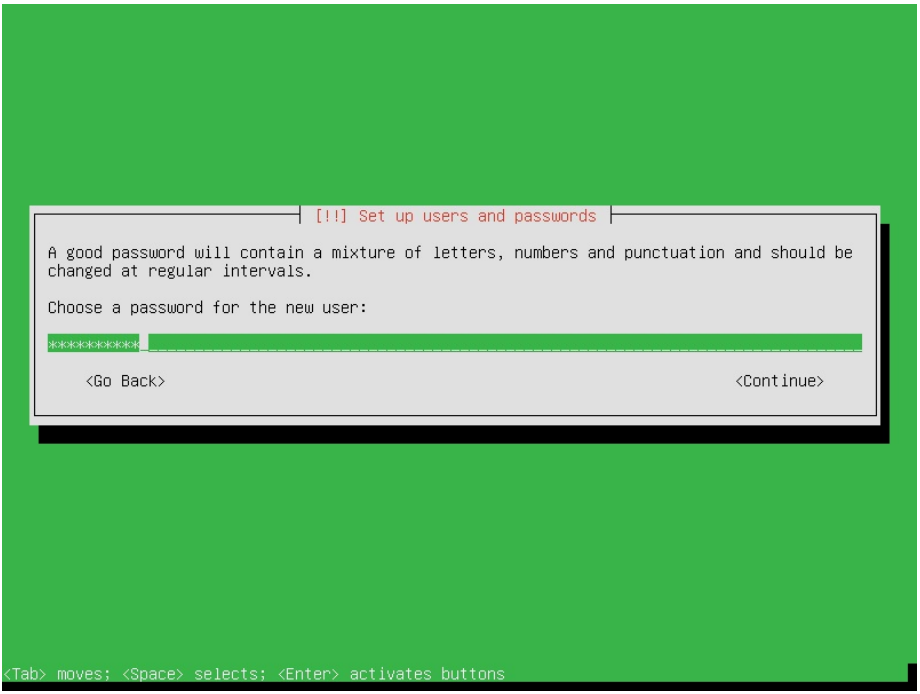
Hostname

Next, the installer will ask you for the administrator account. This user will have administration privileges and in addition, the same user will be used to access the Zentyal interface.

[!!] Set up users and passwords
Select a username for the new account. Your first name is a reasonable choice. The username should start with a lower-case letter, which can be followed by any combination of numbers and more lower-case letters.
Username for your account:
administration
<Go Back>
<Continue>

System username

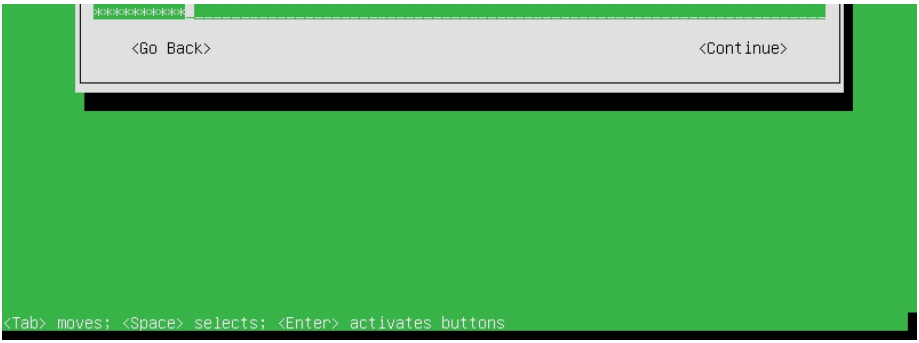
In the next step you are asked for the user password. It is important to note that the user defined earlier, can access, using the same password, both system (via SSH or local *login*) and the Zentyal web interface. Therefore you must be really careful to choose a secure password (more than 12 characters including letters, numbers and symbols).


[!!] Set up users and passwords
A good password will contain a mixture of letters, numbers and punctuation and should be changed at regular intervals.
Choose a password for the new user:
****
<Go Back>
<Continue>
<Tab> moves; <Space> selects; <Enter> activates buttons

Password

Here, insert the password again to verify it.

[!!] Set up users and passwords
Please enter the same user password again to verify you have typed it correctly.
Re-enter password to verify:

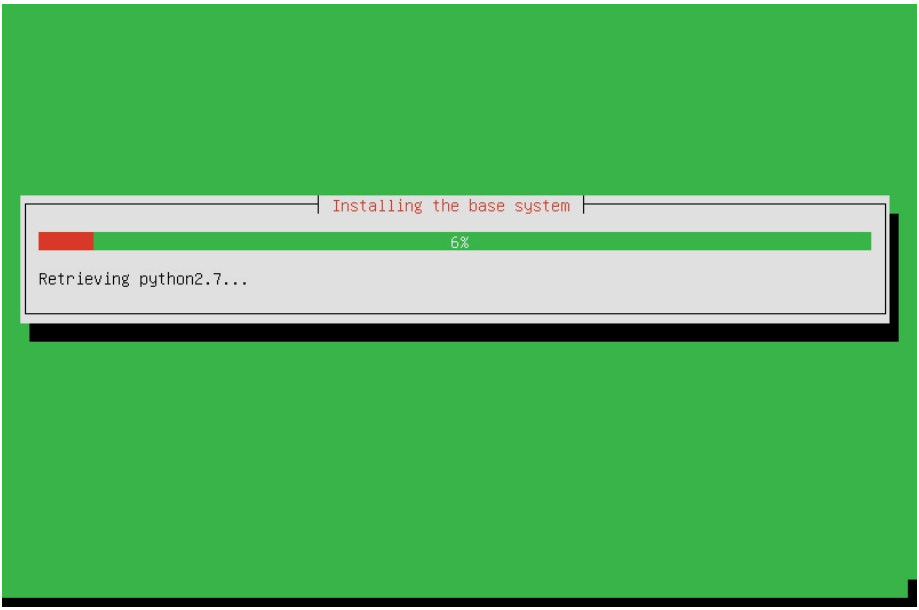


Confirm password

In the next step you are asked for your time zone. It is automatically configured depending on the location chosen earlier, but you can modify it in case this is incorrect.

Time zone

The installation progress bar will now appear. You must wait for the basic system to install. This process can take approximately 20 minutes, depending on the server.

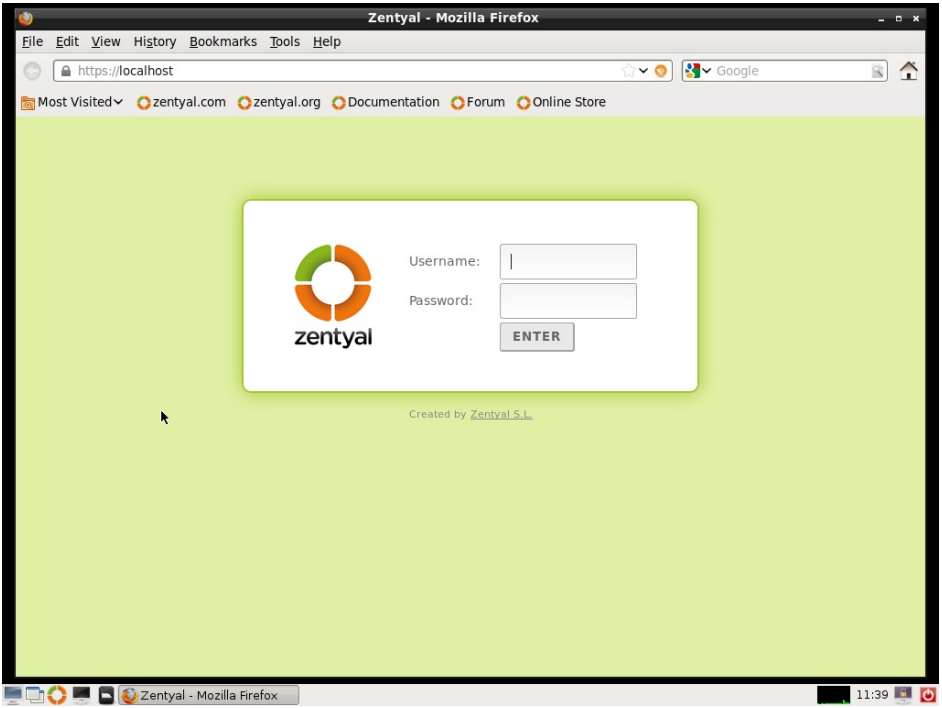


Installation of the base system

Once installation of the base system is completed, you can eject the installation CD and restart the server.

Restart

Now your Zentyal system is installed! A graphical interface in a web browser is started and you are able to access the administrative interface. The first boot will take an extra time while it configures core Zentyal modules. After the first restart, the graphical environment was automatically started, from now on you must authenticate before it begins.



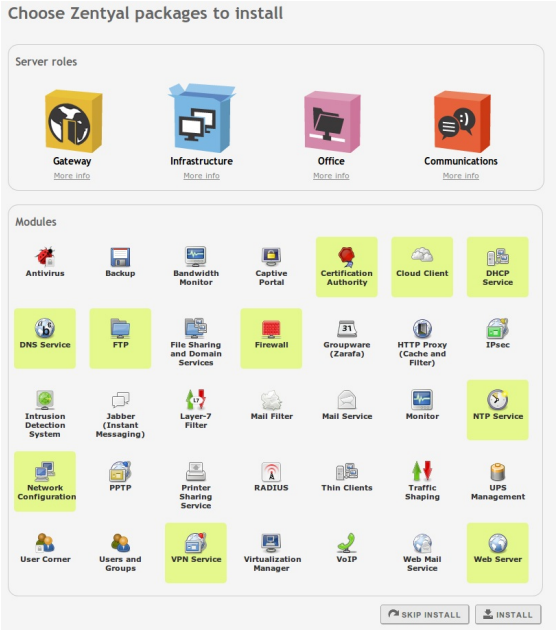
Graphical environment with administrative interface

To start configuring Zentyal profiles or modules, you must insert the username and password indicated during the installation process. Any user you add later to the *sudo* group can access the Zentyal interface and has *sudo* privileges in the system.

[5] LVM is the logical volume manager in Linux, you can find an introduction to LVM management in http://www.howtoforge.com/linux_lvm.

Initial configuration

When you access the web interface for the first time, a configuration wizard will start. To start with, you can choose the functionality for your system. To simplify this selection, in the upper part of the interface you will find the pre-designed server profiles.



Zentyal profiles

Zentyal profiles available for installation:

Zentyal Gateway:

Zentyal will act as a gateway of the local network, offering secure and controlled access to Internet.

Zentyal Infrastructure:

Zentyal manages the infrastructure of the local network with basic services such as DHCP, DNS, NTP, and so on.

Zentyal Office:

Zentyal can act as server for shared resources of the local network: files, printers, calendars, contacts, user profiles and groups.

Zentyal Unified Communications:

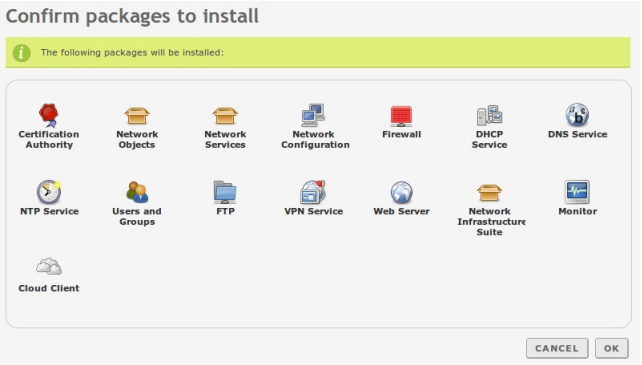
Zentyal can act as a communications center for the company, handling e-mail, instant messaging and VoIP.

You can select any number of profiles to assign multiple roles to your Zentyal Server.

We can also install a manual set of services just clicking on their icons, without having to comply with any specific profile. Another possibility is to install a profile and then manually add the required extra packages.

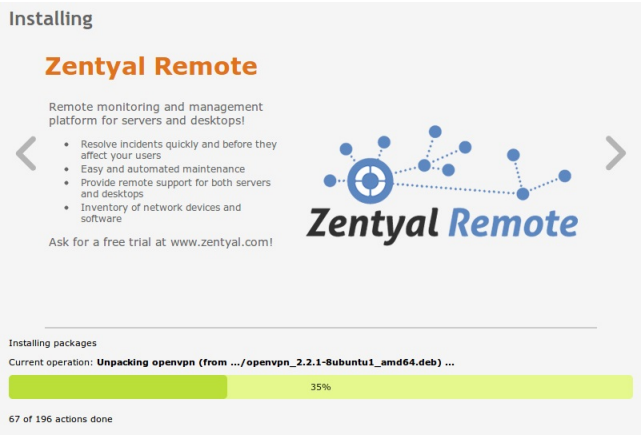
We are going to develop the *Infrastructure* profile in this example. The *wizards* you will see during the installation depend on the packages you have selected to install in this step.

Once you have finished the selection, only the necessary additional packages will be installed. This selection is not definitive and later you can install and uninstall any of the Zentyal modules via the software management tools.



Extra dependencies

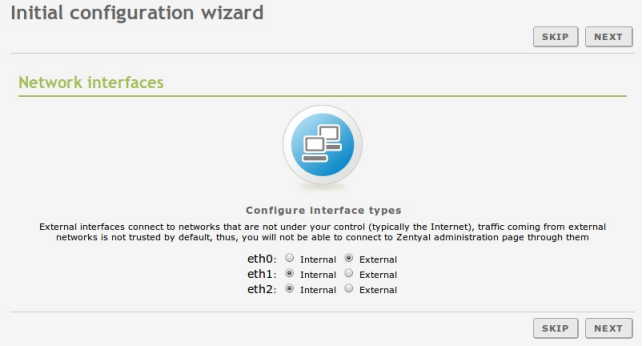
The system will begin the installation process of required modules and you will be shown a progress bar, as well as some slides offering a brief introduction to core Zentyal functions and the commercial packages.


Installing
Zentyal Remote
Remote monitoring and management platform for servers and desktops!
Resolve incidents quickly and before they affect your users
Easy and automated maintenance
Provide remote support for both servers and desktops
Inventory of network devices and software
Ask for a free trial at www.zentyal.com!
Zentyal Remote
Installing packages
Current operation: Unpacking openvpn (from .../openvpn_2.2.1-8ubuntu1_amd64.deb) ...
35%
67 of 196 actions done

Installation and additional information

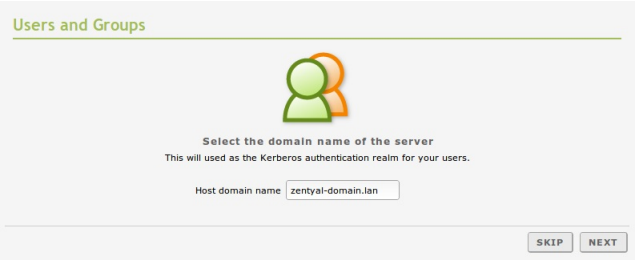
Once the installation process has been completed, the configuration wizard will configure the new modules and then you are asked some questions.

First of all, you are asked for information regarding your network configuration. Then you need to define each network interface as internal or external, in other words; whether it will be used to connect to an external network such as Internet, or to a local network. Strict firewall policies will be applied to all the traffic coming in through external network interfaces.


Initial configuration wizard
SKIP
NEXT
Network interfaces
Configure interface types
External interfaces connect to networks that are not under your control (typically the Internet), traffic coming from external networks is not trusted by default, thus, you will not be able to connect to Zentyal administration page through them
eth0: Internal External
eth1: Internal External
eth2: Internal External
SKIP
NEXT

Initial configuration of network interfaces

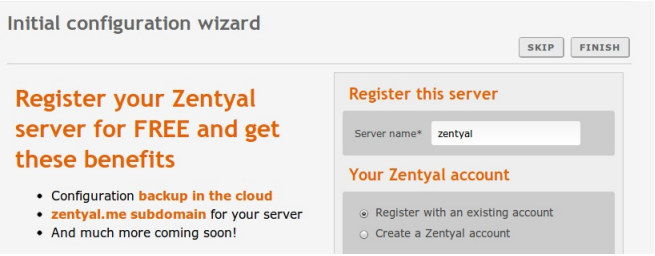
Next, you have to choose the local domain associated with our server, if you have configured the external interface(s) using DHCP it may be filled automatically. As said before, our *hostname* will be automatically added as a *host* of this domain. The authentication domain for the users will also take this name. You can configure additional domains but this is the only one that will come pre-configured to provide all the information that our LAN clients need for the network authentication protocol (Kerberos).

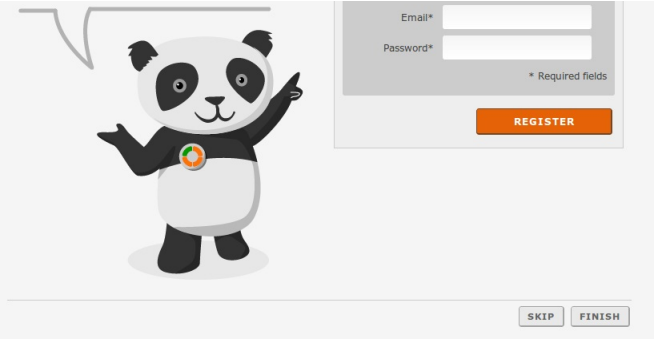


Local domain for the server

The last wizard will allow you to register your server. In case you already have registered, you just need to enter your credentials. If you still don't have registered the server, you can do it now using this form.

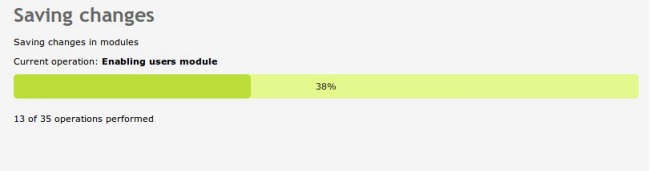
Both ways, the form will request a name for your server. This is the name that will identify your Zentyal server in the *Zentyal Remote* interface.





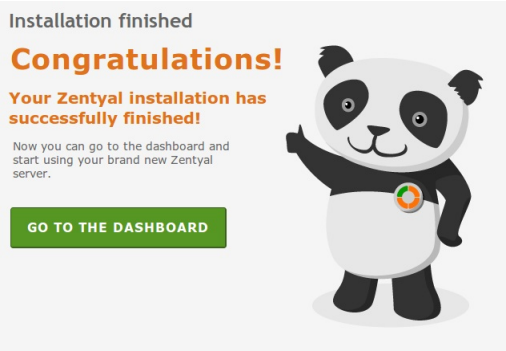
Register your server

Once you have answered these questions, you will continue to configure all the installed modules.



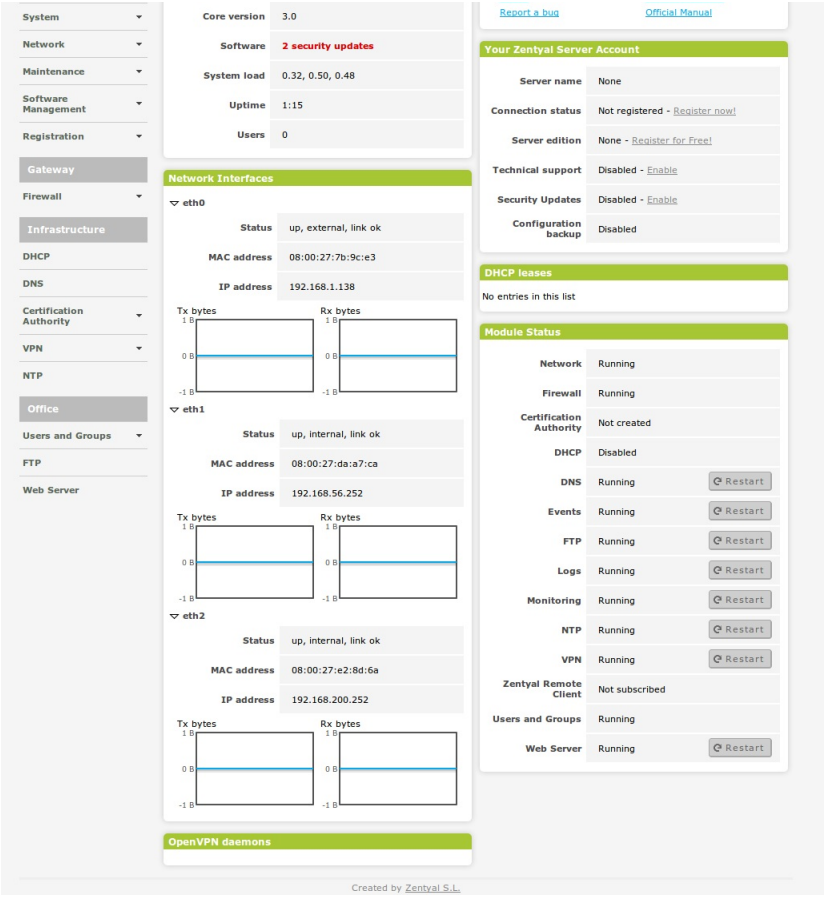
Saving changes

The installer will inform you when the installation is finished.


Installation finished
Congratulations!
Your Zentyal installation has successfully finished!
Now you can go to the dashboard and start using your brand new Zentyal server.
GO TO THE DASHBOARD

Initial configuration is finished

Just click the button and access the *Dashboard*: your Zentyal server is now ready!



Dashboard

Hardware requirements

Zentyal runs on standard x86 or x86_64 (64-bit) hardware. However, you must ensure that Ubuntu Lucid 10.04 LTS (kernel 2.6.32) supports the hardware you are going to use. You should be able to check this information directly from the vendor. Otherwise you can check Ubuntu Linux Hardware Compatibility List [6], list of servers certified for Ubuntu 10.04 LTS [7] or by searching in Google.

The Zentyal server hardware requirements depend on the modules you install. How many users will use the services and what their usage patterns are.

Some modules have low resource requirements, like Firewall, DHCP or DNS. Others, like Mailfilter or Antivirus need more RAM memory and CPU. Proxy and File sharing modules benefit from faster disks due their intensive I/O usage.

A RAID setup gives a higher level of security against hard disk failures and increased speed on read operations.

If you use Zentyal as a gateway or firewall, you will need at least two network cards, but if you use it as a standalone server, one network card is enough. If you have two or more Internet connections, use one network card for each router or connect them to one network card keeping them in the same subnet. VLAN is also an option.

Also, it is always recommended that a UPS is deployed along with the server. For further information see *nut-chapter*

For a general purpose server with normal usage patterns, these are the recommended minimum requirements:

Zentyal Profile	Users	CPU	Memory	Disk	Network cards
Gateway	<50	P4 or equivalent	2G	80G	2 or more
	50 or more	Xeon Dual core or equivalent	4G	160G	2 or more
Infrastructure	<100	P4 or equivalent	1G	80G	1
	100 or more	P4 or equivalent	2G	160G	1
Office	<100	P4 or equivalent	1G	250G	1
	100 or more	Xeon Dual core or equivalent	2G	500G	1
Communications	<100	Xeon Dual core or equivalent	4G	250G	1
	100 or more	Xeon Dual core or equivalent	8G	500G	1

Hardware requirements table

When combining more than one profile, you should think in terms of higher requirements. If you are deploying Zentyal in an environment with more than 100 users, a more detailed analysis should be done including usage patterns, benchmarking and considering high availability strategies.

[6] http://www.ubuntu.com/certification/catalog
[7] http://www.ubuntu.com/certification/release/10.04%20LTS/servers/

Copyright 2004-2012 Zentyal S.L.

First steps with Zentyal

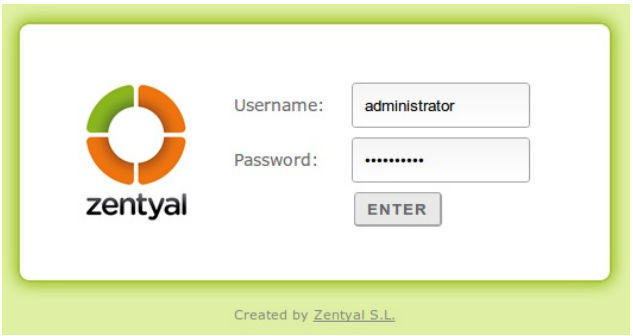
Administrative web interface of Zentyal

Once you have installed Zentyal, you can access to the administrative web interface of Zentyal both through its own graphical environment included in the installer and from anywhere on the internal network, using the address: https://ip_address/, where *ip_address* is the IP address or the hostname on which Zentyal is installed. Because access is through HTTPS, the first time it is accessed the browser will ask you whether you trust the site. You simply accept the self-generated certificate.

Warning: Some older versions of Internet Explorer may have problems accessing the interface. Use the latest version available of your web browser.

Tip: For convenience when using virtualized environments, you should configure a *host-only* network interface in your virtualization solution, so you can access Zentyal's interface full-screen using your native browser. See the example of *Appendix B: Advanced network scenarios*, Scenario 1.

The first screen asks for the username and password. The user created during the installation and any other user of the *admin* group can authenticate as administrator.

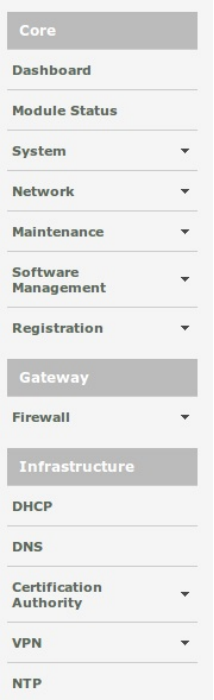


Login

Once authenticated, you will see the administrative interface, this is divided in three main parts:

Left side menu:

Contains links to all the **services** that can be configured by using Zentyal, separated into categories. When you select a service in this menu, a sub menu might appear to configure a particular requirement in the selected service.



Side menu

Top menu:

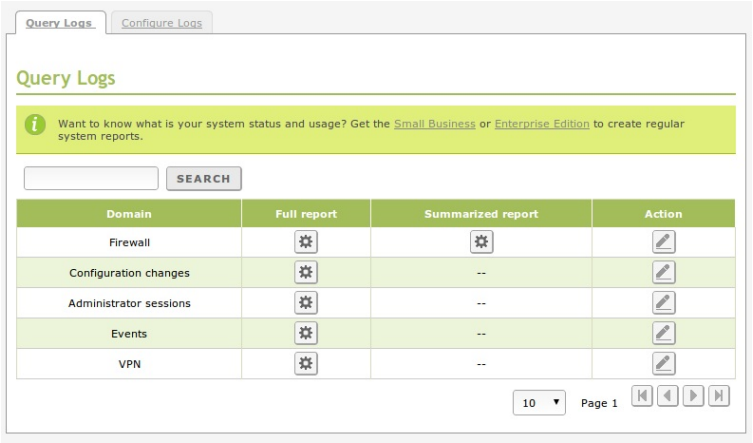
Contains **actions**: save the changes made in the contents to ensure the changes are effective, and log out.

Top menu

Main content:

The content that occupies the central part, consists of one or more forms or tables with information about **service configuration** that are selected through the left side menu and its sub menus. Sometimes, in the top, you can see a bar with tabs: each tab represents a different subsection within the section you have accessed

accessed.



Contents of a form

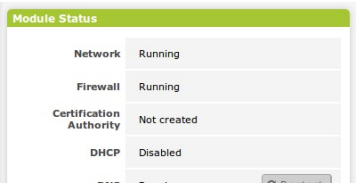
Dashboard

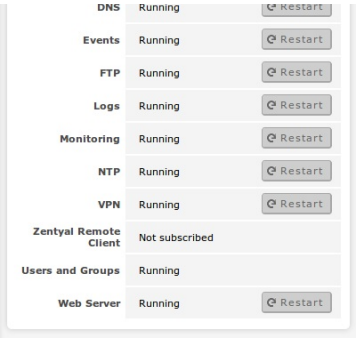
Dashboard is the initial interface screen. It contains a series of *widgets* that can be configured. You can reorganise the widgets at all times by clicking on their titles and dragging them.

By clicking on *Configure Widgets* the interface changes, allowing you to remove and add new *widgets*. To add a new widget, you need to search for it using the top menu and drag it to the central section. To remove a widget, click on the X in the upper right corner of the window.

Dashboard configuration

One of the important *widgets* in the *Dashboard* displays the status of all modules installed on Zentyal.





Widget showing status of the modules

The image shows the status of a service and the action you can carry out for this service. The different statuses are:

Running:

The service is running and listening to client connections. You can restart a service using *Restart*.

Running unmanaged:

If you haven't enabled the module yet, it will be running with the default configuration set by the distribution.

Stopped:

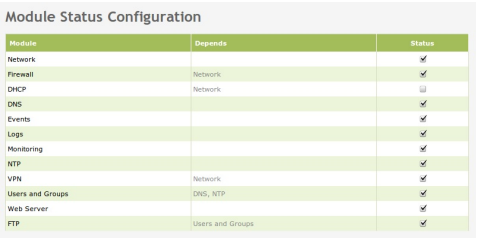
The service is stopped either because the administrator has stopped it or because a problem has occurred. You can restart the service by clicking on *Restart*.

Disabled:

The module has been explicitly disabled by the administrator.

Configuration of the module status

Zentyal uses a modular design in which each module manages a different service. To configure each of these services you must enable the corresponding module from *Module Status*. All those functions that have been selected during the installation will be enabled automatically.

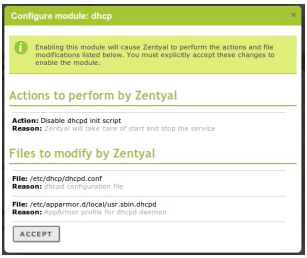


Configuration of the status module

Each module may have dependencies on others modules in order to work. For instance, DHCP module needs to have the network module enabled so that it can serve IP addresses through the configured network interfaces. The dependencies are shown in the *Depends* column and until these are enabled, you can't enable the module.

Tip: It's important to remember that a module will not work until it is activated. Similarly, you can do several changes in a module configuration and they will not apply until you click on *Save Changes*. This behaviour is expected and allows you to carefully double check all the configurations before applying them.

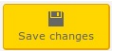
The first time you enable a module, you are asked to accept the set of actions that will be carried out and the configuration files that will be overwritten. After you have accepted all the actions and listed files, you must save changes in order to apply the configuration.


Configure module: dhcp
Enabling this module will cause Zentyal to perform the actions and file modifications listed below. You must explicitly accept these changes to enable the module.
Actions to perform by Zentyal
Action: Disable dhcpd init script
Reason: Zentyal will take care of start and stop the service
Files to modify by Zentyal
File: /etc/dhcp/dhcpd.conf
Reason: dhcpd configuration file
File: /etc/apparmor.d/local/usr.sbin.dhcpd
Reason: AppArmor profile for dhcpd daemon
ACCEPT

Confirmation to enable a module

Applying the configuration changes

An important feature to consider when working with Zentyal is the way configuration changes are applied when made through the interface. Initially, changes must be accepted in the form. Then to make these changes effective and apply them permanently you must click on *Save Changes* in the top menu. This button will change to red if there are any unsaved changes. Failure to follow this procedure will result in the loss of all changes made during the session once you end it. An exception to this rule is the users and groups management: here the changes are applied directly.



Save Changes

Warning: If you change the network interface configurations, firewall or administrative interface port, you might loose the connection. If this is the case you should change the URL in the browser or reconfigure through the local GUI.

General configuration

General configuration

There are several parameters in the general configuration of Zentyal that can be modified in *System* ▸ *General*.

General configuration

Password:

You can change the password of a user. It is necessary to introduce his/her *Username*, *Current password*, *New password* and to confirm the password again in the *Change password* section.

Language:

You can change the interface language using *Select a language*.

Time Zone:

You can specify city and country to adjust your time zone offset.

Date and Time

You can specify the date and time for the server, as long as you are not synchronizing automatically with an external NTP server.

Administrative interface port:

By default, it is the HTTPS port 443, but if you want to use it for the web server, you must change it to another port and specify it in the URL when you access https://ip_address:port/.

Hostname:

It is possible to change the *hostname* or the hostname, for example *zentyal.home.lan*. The hostname is helpful because the server can be identified from other hosts in the same network.

Warning: You have to be careful if you intend to change the machine host name or local domain after the installation, because the authentication configuration (Kerberos) that was automatically performed will no longer be valid. In this case you will have to copy the relevant DNS registers manually.

Network configuration with Zentyal

Through *Network* ▸ *Interfaces* you can access the configuration of each network card detected by the system and you can select between a static configuration (manually configured), dynamic (DHCP configuration), VLAN (802.1Q) trunk, PPoE or *bridged*.

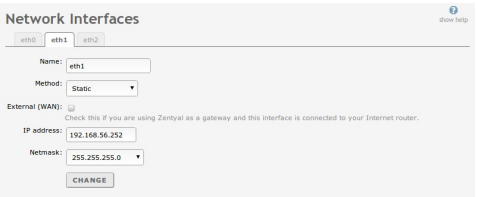
In addition, you can define each interface to be *External* if it is connected to an external network, such as the Internet. In order to apply stricter firewall policies. If you don't do this, the interface is considered internal, connected to a local network.

When you configure an interface to serve DHCP, not only do you configure the IP address, but also the DNS servers and gateway. This is usual for hosts within the local network or for external interfaces connected to the *ADSL routers*.

DHCP configuration of the network interface

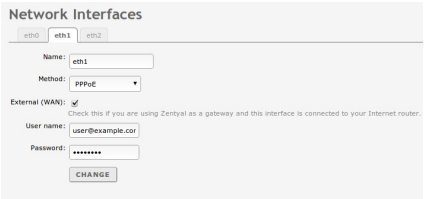
If you decide to configure a static interface you must specify the IP address and the network mask. You can also associate one or more *Virtual Interface* to this real interface to use additional IP addresses.

These additional addresses are useful to provide a service in more than one IP address or sub-network, to facilitate the migration from a previous scenario or to have a web server with different domains using SSL certificates.



Static configuration of the network interface

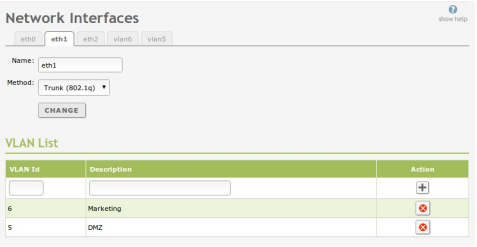
If you use an *ADSL router* PPPoE [1] (a connection method used by some Internet providers), you can also configure these types of connections. To do this, you only have to select *PPPoE* and introduce the *Username* and *Password* supplied by your provider.



PPPoE configuration of the network interface

If you connect the server to one or more VLAN networks, select *Trunk (802.11q)*. Once selected, using this method you can create as many interfaces associated to the defined *tag* as you wish, and consider them as if they were real interfaces.

The VLAN network infrastructure allows you to segment the local network to improve performance and security, without the need to invest in hardware that would usually be necessary to create each segment.



VLAN configuration of the network interface

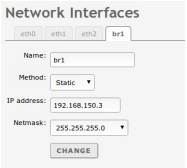
The *bridged* mode consists of associating two physical network interfaces attached to your server that are connected to two different networks. For example, one card connected to the *router* and another card connected to the local network. By using this association you can redirect the network traffic transparently from one card to the other.

The main advantage here, is that client configurations do not need changing when the Zentyal server gateway is deployed. Traffic that passes through the server can be managed using content filtering or the intrusion detection system.

You can create this association by changing the interface with *Bridged network*. You can see how by choosing this option for a new *Bridged network*. Then you can choose the group of interfaces you want to associate to this interface.

Creating a bridge

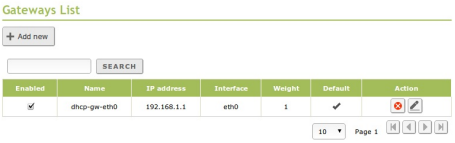
This will create a new virtual interface *bridge* which will have its own configuration as well as a real interface.



Configuring bridged interfaces

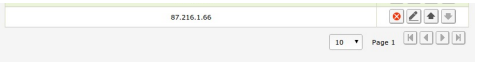
In case you need to configure the network interface manually, define the gateway to Internet using *Network* ▸ *Gateways*. Normally this is automatic if DHCP or PPPoE is in use, but not in other cases. For each gateway you can indicate the *Name*, *IP address*, *Interface* to which it is connected. The *Weight* defines the priority compared with other *gateways* and whether it is *Predetermined* by all of them.

In addition, if an HTTP proxy is required for Internet access, you can also configure this in this section. This proxy will be used by Zentyal for connections, such as updates and the installation of packages or the update of the anti-virus data files.



Configuration of gateways

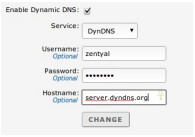
To allow the system to resolve domain names, you must indicate the address of one or several name servers in *Network* ▸ *DNS*.



Configuration of DNS servers

If the Internet connection assigns a dynamic IP address and you need a domain name to re-direct, you need a provider of dynamic DNS. By using Zentyal you can configure some of the most popular providers of dynamic DNS.

To do this, you must select *Network* ▸ *DynDNS* where you can choose the *Service* provider, *Username*, *Password* and *Hostname* which needs updating when the public address changes. Finally select *Enable dynamic DNS*.



Configuration of Dynamic DNS

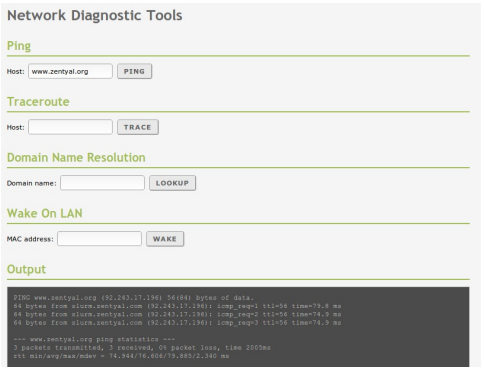
Zentyal connects to a provider to obtain a public IP address avoiding any translation of the network address (NAT) between the server and Internet. If you are using this feature in the *multirouter* [2] scenario, you must not forget to create a rule to ensure the connections to the provider always use the same gateway.

[1] http://en.wikipedia.org/wiki/PPPoE

Network diagnosis

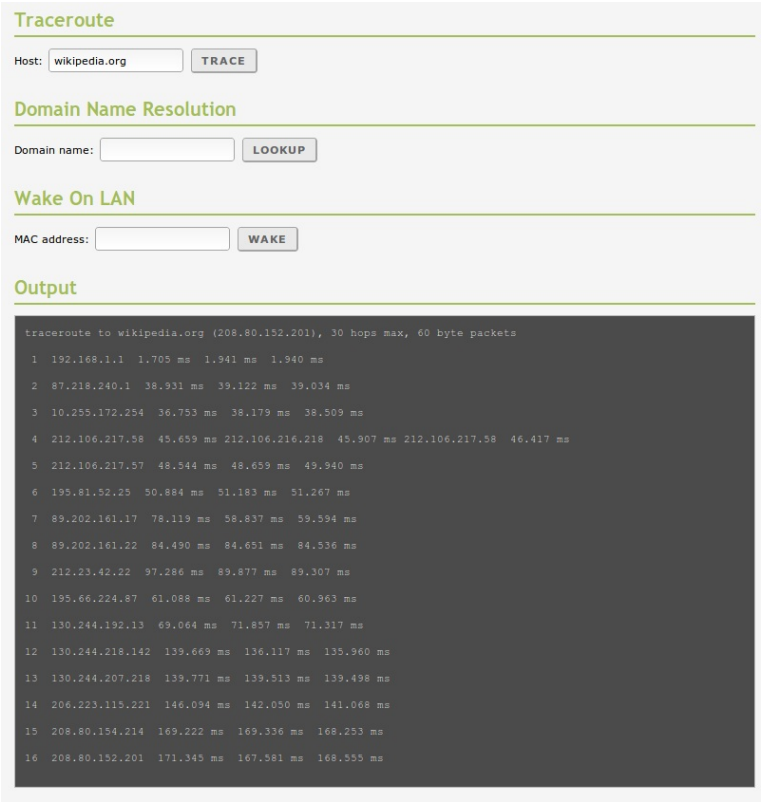
To check that the network has been configured correctly, you can use the tools available in *Network* ▸ *Tools*.

Ping is a tool that uses the ICMP network diagnosis protocol to observe whether a particular remote host is reachable by means of a simple “echo request”.



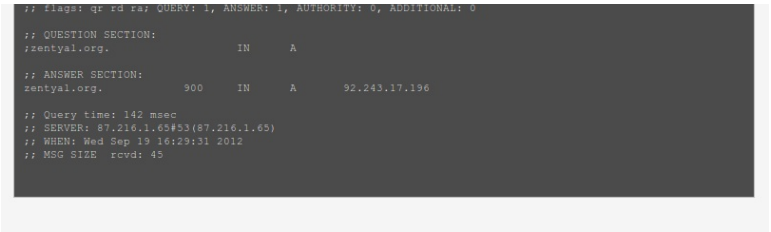
Network diagnosis tools, ping

You can also use the **traceroute** tool that is used to determine the route taken by packages across different networks until they reach a given remote host.



Tool traceroute

Also, you can use the **domain name resolution** tool, which is used to verify the correct functioning of the name service.


;; flags: qr rd ra; QUERY: 1, ANSWER: 1, AUTHORITY: 0, ADDITIONAL: 0
;; QUESTION SECTION:
;zentyal.org. IN A
;; ANSWER SECTION:
zentyal.org. 900 IN A 92.243.17.196
;; Query time: 142 msec
;; SERVER: 87.216.1.65#53(87.216.1.65)
;; WHEN: Wed Sep 19 16:29:31 2012
;; MSG SIZE rcvd: 45

Domain name resolution

The last tool is *Wake On Lan*, which allows you to activate a host using its *MAC* address, if this feature is enabled in the target.

Copyright 2004-2012 Zentyal S.L.

Software updates

Like any other software system, Zentyal server requires periodic updates, either to add new features or to fix defects or system failures.

Zentyal distributes its software as packages and it uses Ubuntu's standard tool, **APT** [1]. However, in order to ease this task, a web interface is provided to simplify the process. [2]

[1] *Advanced Packaging Tool* (APT) is a system for the management of software packages created by the Debian Project which greatly simplifies the installation and removal of programs on Linux http://wiki.debian.org/Apt

[2] For a more extensive explanation on how to install software packages in Ubuntu, please read the chapter on package management in Ubuntu's official documentation https://help.ubuntu.com/12.04/serverguide/C/package-management.html

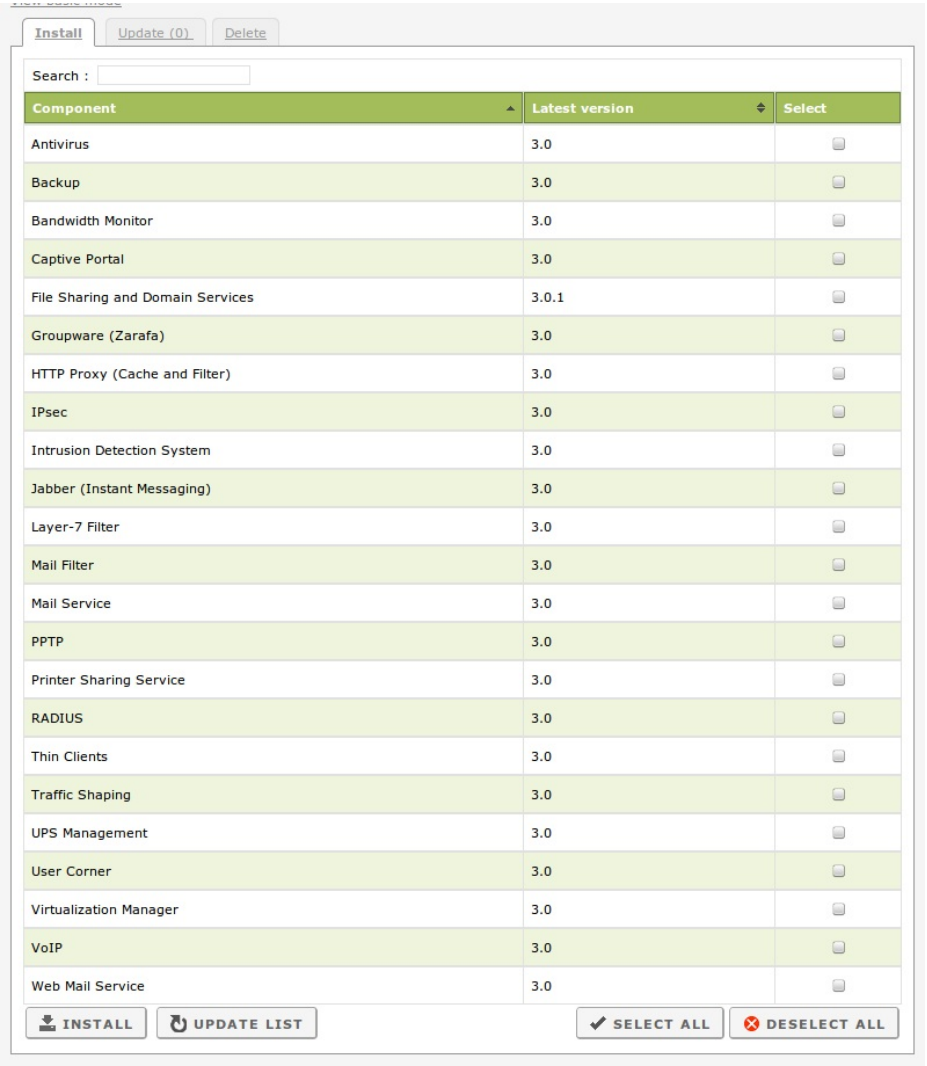
The web interface allows checking for new available versions of Zentyal components and installing them in a simple way. It also allows you to update the software supporting Zentyal, mainly to correct potential security flaws.

Management of Zentyal components

The **management of Zentyal components** allows you to install, update and delete Zentyal modules.

To manage Zentyal components you must access *Software Management -> Zentyal components*.

View basic mode



Management of Zentyal components

When entering this section you will see the advanced view of the package manager, that you might have seen already during the installation process. This view has three tabs, each one for the actions of *Installing*, *Updating* and *Deleting* Zentyal components.

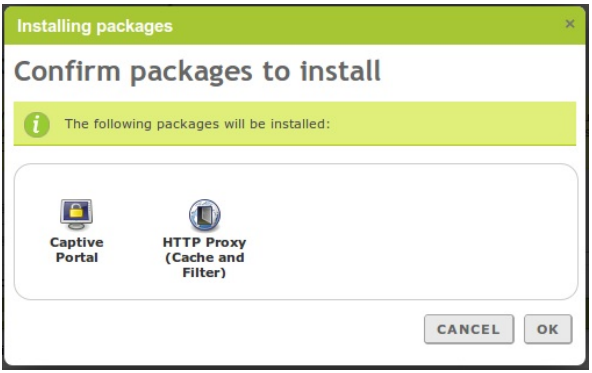
On this view, there is an option to change to *basic mode*, on which you can install package collections depending on the role of the server you are setting up.

Getting back to the advanced view, let's see the available action in detail.

Component installation

Tab is visible when you enter in the component management section. There are three columns here, one for the component name, another for the version currently available in the repositories and a third to select the component. In the lower part of the table you can view the buttons to *Install*, *Update list*, *Select all* and *Deselect all*.

To install the required components, simply select them and click on the *Install* button. You will then be taken to a page with a complete list of the packages to be installed.



Confirm the installation

The *Update list* button synchronises the list of packets with the repositories.

Component update

The following tag, *Update*, shows between brackets the number of available updates. Apart from this feature, this section is organised in a similar way to the installation view, with only some minor differences. An additional column indicates the version currently installed and in the bottom of the table you can see a button which can be clicked to select packages to upgrade. As with the installation of components, you will see a confirmation screen showing the packages to be updated.

Component deletion

The last tag, *Delete*, shows a table with the installed packages and their versions. In a similar way as with the previous view, you can select packages to uninstall and then, to complete the action click the *Delete* button in the lower left part of the table to complete the action.

Before performing the action, just like in previous examples, Zentyal will ask for confirmation before deleting the selected packages and their dependencies.

System Updates

The **system updates** section performs the updating of third party software used by Zentyal. These programs are referenced as **dependencies**, ensuring that when installing Zentyal, or any of the required modules, they are also installed. This guarantees the correct operation of the server. Similarly, these programs may have dependencies too.

Usually the update of a dependency is not important enough to create a new Zentyal package with new dependencies, but it may be useful to install it in order to use its improvements or its patches to fix security flaws.

To see the system updates you must go to *Software Management* ▸ *System Updates*. Here you can see if your system is already updated or, otherwise, a list of packages that can be upgraded is displayed. If you install packages on the server without using the web interface, this data may be outdated. Therefore, every night a process is executed to search for available updates for the system. A search can be forced by clicking on the button *Update list* on the lower part of the page.

Component	Description	Version	Update
linux-generic	Complete Generic Linux kernel	3.2.0.30.32	☐
linux-generic	Complete Generic Linux kernel	3.2.0.30.32	☐
linux-firmware	Firmware for Linux kernel drivers	1.79.1	☐
linux-firmware	Firmware for Linux kernel drivers	1.79.1	☐
linux-image-generic	Generic Linux kernel image	3.2.0.30.32	☐
linux-image-generic	Generic Linux kernel image	3.2.0.30.32	☐
gpgv	GNU privacy guard - signature verification tool	1.4.11-3ubuntu2.1	☐
gpgv	GNU privacy guard - signature verification tool	1.4.11-3ubuntu2.1	☐
resolvconf	name server information handler	1.63ubuntu16	☐

System Updates

For each update, you can determine whether it is a security update using the information icon. If it is a security update the details about the security flaw included in the package changelog will be displayed by clicking on the icon.

If you want to perform an update, select the packages on which to perform the action and press the appropriate button. As a shortcut, the button *Update all packages* can be used. Status messages will be displayed during the update operation.

Automatic updates

Automatic updates allow Zentyal server to automatically install any updates available.

This feature can be enabled by accessing the page *Software Management -> Settings*.

Automatic updates management

On that page you can also choose the time of the day during which these updates will be performed.

It is not advisable to use this option if the administrator needs to keep a higher level of security and control for the management of updates.

Copyright 2004-2012 Zentyal S.L.

Zentyal Remote Client

About Zentyal Remote

Zentyal Remote is a solution that provides automatic maintenance of servers, as well as real-time monitoring and centralised management of multiple Zentyal installations. It offers features such as; quality assured software updates, alerts and reports on server performance, network inventory, security audits, disaster recovery, advanced security updates, network monitoring and remote, centralised and secure management of groups of servers, as well as the remote access and inventory for desktop. [1]

If you don't have a Zentyal server commercial edition, you can still register your community server. This entitles you to store one remote configuration backup, create zentyal.me subdomain for your server and to see your Zentyal server name in the web browser tab.

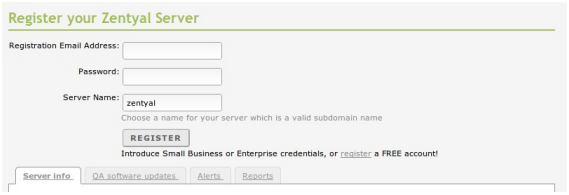
In the following pages, you will learn how to register your server to Zentyal Remote with a community server and you will see the additional functionality that a registered server offers. Please remember that Zentyal servers in production environments should always have commercial editions to guarantee maximum security and system uptime. [2]

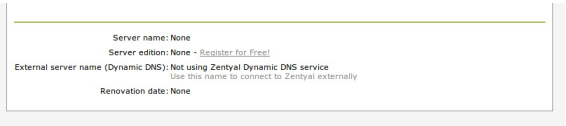
[1] http://www.zentyal.com/services/
[2] http://www.zentyal.com/which-edition-is-for-me/

Registering Zentyal server to Zentyal Remote

To register your Zentyal server to Zentyal Remote, you must first install the *Zentyal Remote Client* component. This is installed by default if you used Zentyal installer. In addition to this, Internet connection should be available. You can register your server during installation or later from the *Registration* ‣ *Server Registration* menu.

By default, you will see the form to enter the credentials of an existing account. If we want to create a new account, we can go to the installation *wizard* by clicking on the *register a free account* underneath the register button.




Server name: None
Server edition: None - Register for Free!
External server name (Dynamic DNS): Not using Zentyal Dynamic DNS service
Use this name to connect to Zentyal externally
Renovation date: None

Enter the credentials for the existing account

Registration Email Address:

You must set the user name or the email address you use to sign in the Zentyal Remote Web site.

Password:

The same password you use to sign in the Zentyal Remote Web site.

Zentyal name:

A unique name for this server that will be used within the Zentyal Remote. This name is displayed in the control panel and it must be a valid domain name. Each server should have a different name; if two servers use the same name for connecting Remote, only one will be able to connect.

The *Server name* field will be used as the title of the administration webpage of this Zentyal server, so you can quickly check which hosts you are using if you have several interfaces open at the same time in your browser. Additionally, this 'hostname' will be added to the dynamic domain 'zentyal.me', thus, using the address '<yourzentyal>.zentyal.me' you can connect both to the administration page and the SSH console (as long as you have allowed this type of connections in your Firewall).

After you have entered your data, click on the Registration button: The registration will take around a minute to complete. It will save changes along this process, thus it is recommended to register your server without changes to apply. During the registration process, a VPN connection between the server and Zentyal Remote may be established (if you have Remote Access Support), thus, the **VPN** [3] module will be enabled.

[3] For more information about VPN, see the *Virtual private network (VPN) service with OpenVPN* section.

If the registration process went fine, then you will be able to see a *widget* on the *dashboard* with the following info.

Your Zentyal server account *Widget*

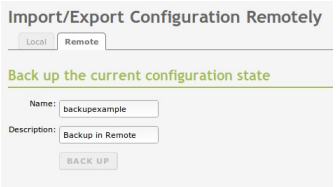
There you are able to see the server edition and the rest of the purchased services, if any, in this widget.

Configuration backup in Zentyal

Remote

One of the features of Zentyal Remote is automatic configuration backup of your Zentyal server, stored in the cloud. If you register your community server, then you can save one configuration backup remotely. If you have a commercial edition (Small Business or Enterprise Subscription), you can save up to seven different configuration backups.

The configuration backup is made on a daily basis if there is any change in Zentyal server configuration. You can do this from *System – > Import/Export configuration* and then clicking on the tab *Remote*. You can make manual configuration backups if you want to make sure there is a backup of your last configuration changes.



Remote configuration backup

You can restore, download or delete the configuration backups that are stored in Zentyal Remote.

Other services along with your registration

Hostname in browser tab

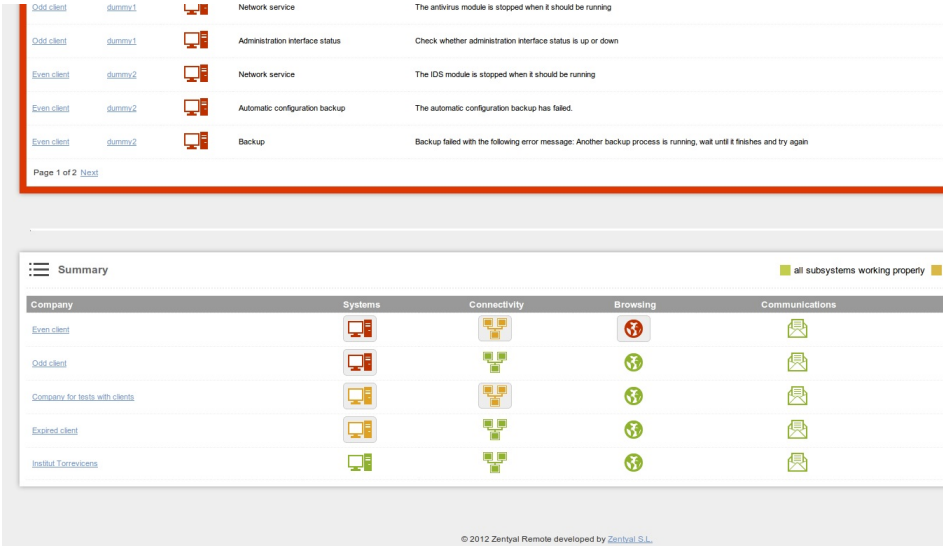
Notice the Zentyal servers by their name in the web browser tab. This is useful if you manage several Zentyal servers from the same browser.

Hostname added to dynamic domain zentyal.me

A zentyal.me subdomain for your server with multigateway support and with up to 3 aliases.

Zentyal Remote access

Once our server is registered, you may access to the Zentyal Remote site [4] and log in with the account we have registered and we may see the following welcome page.


Odd client dummy1 Network service The antivirus module is stopped when it should be running
Odd client dummy1 Administration interface status Check whether administration interface status is up or down
Even client dummy2 Network service The IDS module is stopped when it should be running
Even client dummy2 Automatic configuration backup The automatic configuration backup has failed.
Even client dummy2 Backup Backup failed with the following error message: Another backup process is running, wait until it finishes and try again
Page 1 of 2 Next
Summary
all subsystems working properly
Company
Systems
Connectivity
Browsing
Communications
Even client
Odd client
Company for tests with clients
Expired client
Institut Torrevicens
© 2012 Zentyal Remote developed by Zentyal S.L.

Panel web de Zentyal Remote

[4] https://remote.zentyal.com

Please note that registering your server gives you access only to a limited set of Zentyal Remote features. For information about the features included in the Small Business and Enterprise Editions, check out the Zentyal website [5] or Zentyal Remote documentation [6].

[5] http://www.zentyal.com/which-edition-is-for-me/

[6] https://remote.zentyal.com/doc/

Copyright 2004-2012 Zentyal S.L.

Zentyal Infrastructure

This section explains several of the services used to manage the infrastructure of your local network and to optimise internal traffic. We will study Zentyal's high-level abstractions, the objects and services that will be used in most of the other modules, name domain management, time synchronisation, automatic network configuration, deployment of thin clients, the management of a certification authority and the different types of virtual private networks you can deploy and installing virtual machines.

Defining abstractions will help you manage the entities that will be used by the other modules, creating a coherent and robust context.

Domain Name System or DNS provides access to services and hosts using names instead of IP addresses, these are easier to memorise.

The Network Time Protocol or NTP, keeps the system time synchronised on the different computers within a network.

The DHCP service is widely used to automatically configure different network parameters on computers such as; IP address, DNS servers or the gateway which is used to access to the Internet.

The Thin Client module (LTSP) allows you to reuse old hardware, creating a centralized management infrastructure where a lot of low-end terminals are powered by a few higher-end servers.

The growing importance of ensuring the authenticity, integrity and privacy of communications has increased interest in the deployment of

privacy of communications has increased interest in the deployment of certification authorities. These facilitate access to various services in a safe way. Certificates allow configuration of SSL or TLS to securely access most services and provided certificates for user authentication.

By using VPN (Virtual Private Network), it is possible to interconnect different private subnets via the Internet in a completely safe way. A typical example of this feature is the communication between two or more offices of the same company or organisation. You can also use VPN to allow users to connect remotely and securely to the corporate network.

In addition to the *openvpn* protocol, Zentyal offers you the *IPSec* and *PPTP* protocols to ensure compatibility with third party devices and windows boxes where you do not want to install additional software.

Sometimes, your deployment requires a few applications that can't be ported to Linux environments given their characteristics or age. The Virtual Machines module offers you a way to integrate virtualized services in a simple, elegant and transparent way to the final user.

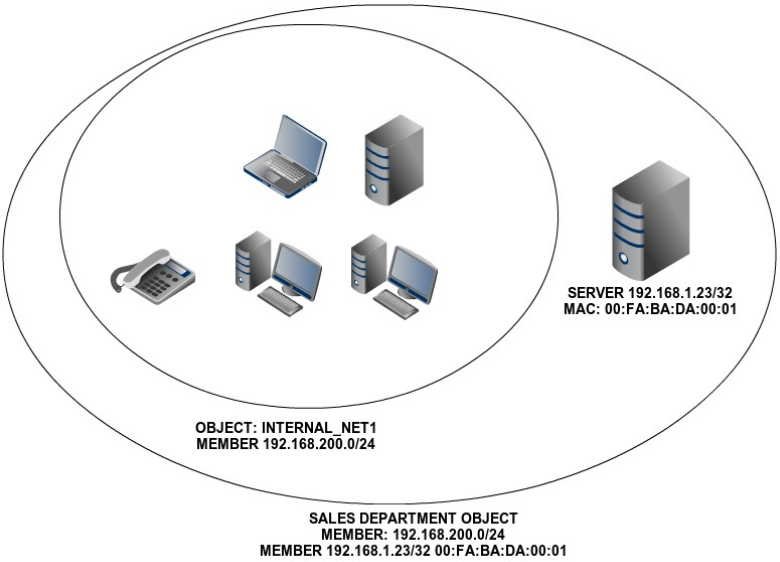
Copyright 2004-2012 Zentyal S.L.

High-level Zentyal abstractions

Network objects

Network objects represent network elements, or a group of them. They allow you to simplify and consequently make it easier to manage network configuration: network objects allow you to give an easily recognisable name to elements or a group of them. This means you can apply the same configuration to all elements.

For example, instead of defining the same firewall rule for each IP address of a subnetwork, you could simply define it for the network object that contains the addresses.

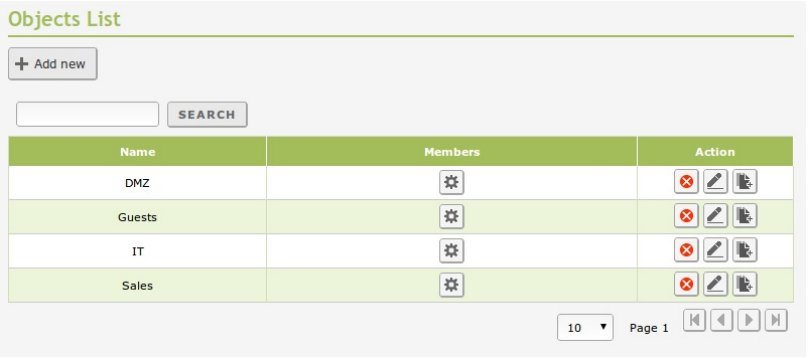


Representation of network objects

An object consists of any number of members. Each member consists of a network range or a specific host.

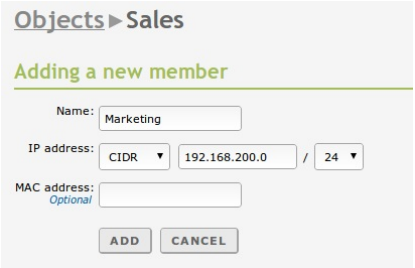
Management of Network objects with Zentyal

To start working with the Zentyal objects, go to *Network* ▸ *Objects* section. Initially you will see an empty list; with the name of all the objects and a series of actions you can carry out on each of them. You can create, edit and delete objects that will be used later by other modules.



Network objects

Each one of these objects consists of a series of members that can be modified at any time. The members must have at least the following values: *Name*, *IP Address* and *Netmask*. The *MAC address* is optional, you can only use it on members that represent a single host. This value will be applied when the MAC address is accessible.



Add a new member

The members of one object can overlap with members of other objects. This is very useful to establish arbitrary groups, but you have to

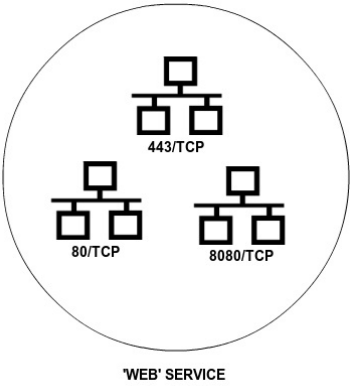
This is very useful to establish arbitrary groups, but you have to consider them when using the rest of the modules to obtain the wanted configuration and to avoid conflicts.

In other configuration sections of Zentyal where you can use network objects (like DHCP or Firewall), a quick embedded menu will be offered, so you can create and configure the network objects without explicitly accessing this menu section.

Network services

Network services is a way to represent the protocols (TCP, UDP, ICMP, etc) and the ports used by an application or a group of related applications. The purpose of the services is similar to that of the objects: objects simplify reference to a group of IP addresses with a recognisable name. Services allows identification of a group of ports by the name of the services the ports have been allocated to.

When browsing, for example, the most usual port is the HTTP port 80/TCP. But in addition, you also have to use the HTTPS port 443/TCP and the alternative port 8080/TCP. Again, it is not necessary to apply a rule that affects the browsing of each one of the ports, but the service that represents browsing and contain these three ports. Another example is the file sharing in Windows networks, where the server listens to the ports 137/TCP, 138/TCP, 139/TCP and 445/TCP.

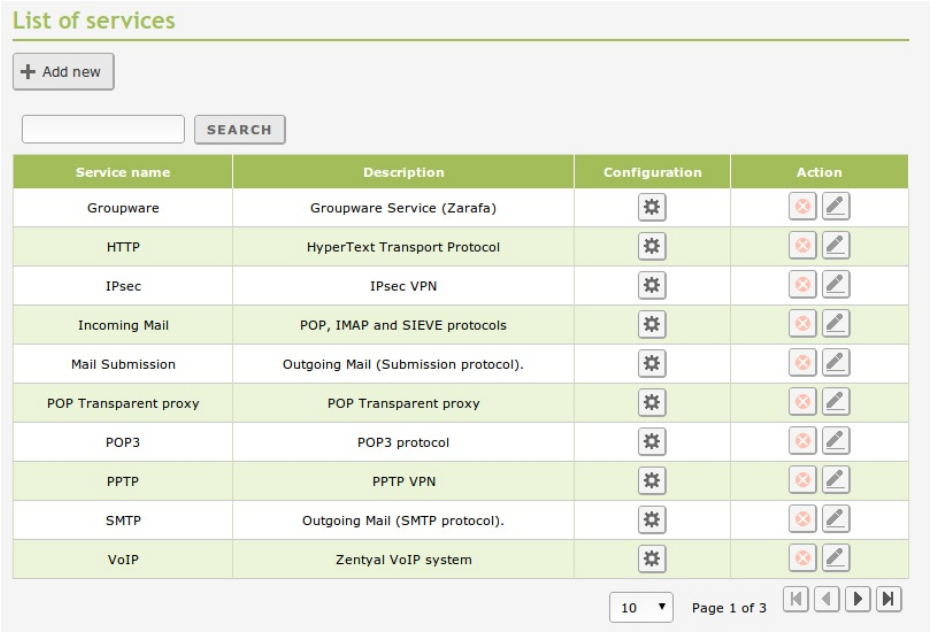


Example of a service composed of different ports

Management of Network services with

To manage services with Zentyal, go to *Network* ▸ *Services* menu, where you will find a list of available services, created by all the installed modules and those that were added later. You can see the *Name*, *Description* and access the *Configuration*. Furthermore, each service has a series of members; each one contains *Protocol*, *Source port* and *Destination port* values. You can introduce the value *Any* in all of the fields to specify, for example, the services for which the source port is different to the destination port.

TCP, UDP, ESP, GRE or ICMP protocols are supported. You can also use a TCP/UDP value to avoid having to add the same port twice when both protocols are used by a service, for example DNS.



Network services

Copyright 2004-2012 Zentyal S.L.

Domain Name System (DNS)

DNS configuration is vital to the functioning of the local network authentication (implemented with Kerberos since the Zentyal 3.0 version), the network clients query the local domain, their SRV and TXT records to find servers with ticket authentication. As mentioned before, this domain is preconfigured to resolve Kerberos services since the installation. For additional information regarding directory services, check *Directory Service (LDAP)*.

BIND [4] is the *de facto* DNS server on the Internet, originally developed at the University of California, Berkeley and currently maintained by the *Internet Systems Consortium*. BIND version 9, rewritten from scratch to support the latest features of the DNS protocol is used by Zentyal's DNS module.

[4] http://www.isc.org/software/bind

DNS cache server configuration with Zentyal

Zentyal's DNS module always works as a DNS cache server for networks marked as internal, so if you only want your server to perform cache DNS queries, simply enable the module.

Sometimes, this DNS cache server might need to be queried from internal networks that are not directly configured in Zentyal. Although this case is quite rare, it may occur in networks with routes to internal segments or VPN networks.

Zentyal allows configuration of the DNS server to accept queries from these subnets by a configuration file. You can add these networks to the file `/etc/zentyal/80dns.conf` with the option *intnets*=:

```
# Internal networks allowed to do recursive queries
# to Zentyal DNS caching server. Localnetworks are alr
# allowed and this settings is intended to allow netwo
# reachable through static routes.
# Example: intnets = 192.168.99.0/24,192.168.98.0/24
intnets =
```

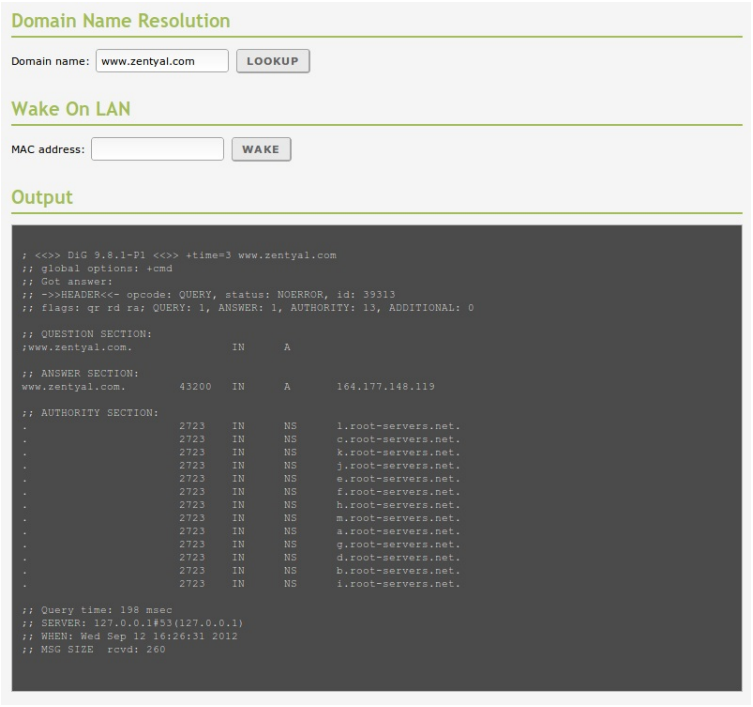
After restarting the DNS module the changes will be applied.

Zentyal's DNS cache server will query root DNS servers directly to find out which authoritative server will solve each DNS request. Then it will store the data locally during the time period set in the *TTL* field. This feature reduces the time required to start every network connection, giving the users a sensation of speed and reducing the overall Internet traffic.

The search domain is basically a string that is added to a search in case a user defined string is unresolvable. The search domain is set on the clients, but it can be provided automatically by DHCP, so that when the clients receive the initial network configuration, they can also receive the search domain.

For example, your search domain could be *foocorp.com*. When a user tries to access the host *example*; as it is not present among its known hosts, the name resolution will fail, then the user's operating system will automatically provide *example.foocorp.com*, resulting in successful name resolution.

In *Network ▸ Tools* you have a tool for *Domain Name Resolution*, which by using *dig* shows the details of a DNS query to the server you have set in *Network ▸ DNS*.

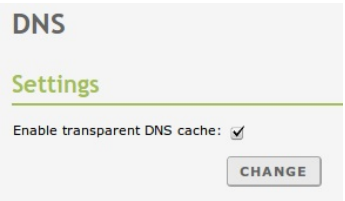

Domain Name Resolution
Domain name: www.zentyal.com
LOOKUP
Wake On LAN
MAC address:
WAKE
Output
; <<>> DiG 9.8.1-P1 <<>> +time=3 www.zentyal.com
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 39313
;; flags: qr rd ra; QUERY: 1, ANSWER: 1, AUTHORITY: 13, ADDITIONAL: 0
;; QUESTION SECTION:
;www.zentyal.com. IN A
;; ANSWER SECTION:
www.zentyal.com. 43200 IN A 164.177.148.119
;; AUTHORITY SECTION:
. 2723 IN NS l.root-servers.net.
. 2723 IN NS c.root-servers.net.
. 2723 IN NS k.root-servers.net.
. 2723 IN NS j.root-servers.net.
. 2723 IN NS e.root-servers.net.
. 2723 IN NS f.root-servers.net.
. 2723 IN NS h.root-servers.net.
. 2723 IN NS m.root-servers.net.
. 2723 IN NS a.root-servers.net.
. 2723 IN NS g.root-servers.net.
. 2723 IN NS d.root-servers.net.
. 2723 IN NS b.root-servers.net.
. 2723 IN NS i.root-servers.net.
;; Query time: 198 msec
;; SERVER: 127.0.0.1#53(127.0.0.1)
;; WHEN: Wed Sep 12 16:26:31 2012
;; MSG SIZE rcvd: 260

Domain name resolution using the DNS local cache

Transparent DNS Proxy

Transparent DNS Proxy

Zentyal's **transparent DNS Proxy** gives you a way to force the use of your DNS server without having to change the clients' configuration. When this option is enabled, all the DNS requests that are routed through your server are redirected to Zentyal's internal DNS server. The clients have to use Zentyal as its gateway to make sure the requests will be forwarded. To have this option available, the **firewall** module must be enabled.



Transparent DNS proxy

DNS Forwarders

The **redirectors** or **forwarders** are DNS servers that your server will query. First your server will search in the local cache, among the registered domains and previously cached queries; in case there is no answer, it will query the redirectors. For example, the first time you query www.google.com, Zentyal's DNS server will query redirectors and store the request in cache if the domain google.com is not registered to your server.

DNS Forwarders

In case forwarders are not configured, Zentyal's DNS server will use the DNS root servers [5] to solve queries that are not stored.

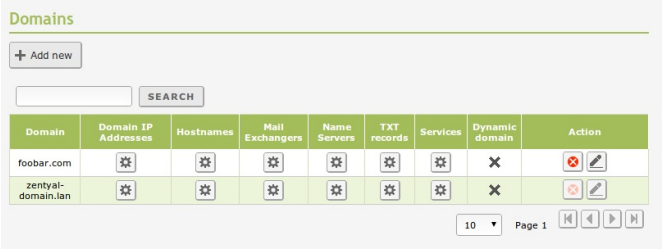
[5] http://en.wikipedia.org/wiki/Root_name_server

Configuration of an authoritative DNS server with Zentyal

In addition to DNS cache, Zentyal can act as an authoritative DNS

In addition to DNS cache, Zentyal can act as an authoritative DNS server for a list of configured domains. As an authoritative server, it will respond to queries about these domains coming both from internal and from external networks, so that not only local clients, but anyone can resolve these configured domains. Cache servers only respond to queries from internal networks.

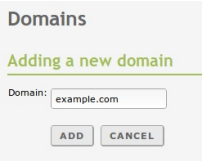
The configuration of this module is done through the *DNS* menu, where you can add as many domains and subdomains as required.



List of domains

See the "local" domain set during the installation or later through the DNS wizard. One of the TXT records of this domain contains a Kerberos authentication *realm* (concept similar to that of domain). In the service records (SRV) you can find information about the hosts and ports required for user authentication. Again, if you decide to remove this domain, it would be useful to replicate this information in the new domain. You can have simultaneously all the domains you want: this will not cause any problem for the previously mentioned authorization methods.

To configure a new domain, display the form by clicking on *Add new*. You can configure the *Domain name* from here.

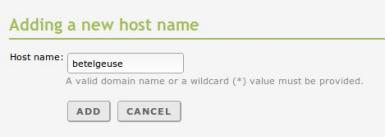


Adding a new domain

You will see that within the domain you can configure different names: in the first place the *IP Addresses of the domain*. A typical case is to add all Zentyal IP addresses to the local network interfaces as IP addresses of the domain.

Once the domain has been created, you can define as many names (Type A) as required within the table *Hostnames*. For each one of these names Zentyal will automatically configure reverse resolution. Moreover, for each name you can define as many *Alias* as necessary. Again, you can associate more than one IP address to your hostname,

that can help the clients to balance between different servers, for example, two replicated LDAP servers with the same information.



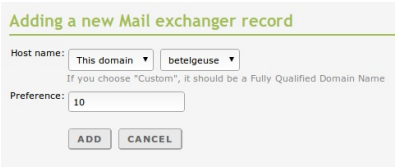
Adding a host

Normally the names point to the host where the service is running and the aliases to the services hosted. For example, the host *amy.example.com* has the aliases *smtp.example.com* and *mail.example.com* for mail services and the host *rick.example.com* has the aliases *www.example.com* and *store.example.com*, among others, for web services.

> **Tip:** When you add hosts or host's alias to a domain, the domain name itself it's implicit. So you will add 'www', not 'www.domain.example'.

Adding a new alias

Additionally, you can define the mail servers responsible for receiving messages for each domain. In *Mail exchangers* you will choose a server from the list defined at *Names* or an external list. Using *Priority*, you can set the server that will attempt to receive messages from other servers. If the preferred server fails, the next one in the list will be queried.

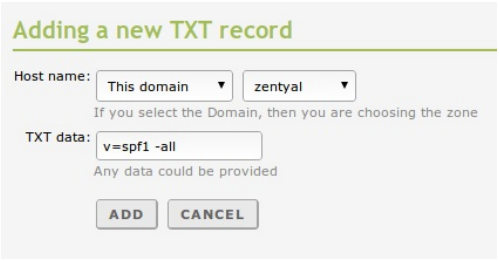


Adding a new mail exchanger

It is also possible to set *NS* records for each domain or subdomain using the table *Name servers*.

Adding a new name server

T h e **text records** are DNS registers that will offer additional information about a domain or a hostname using plain text. This information could be useful for human use or, more frequently, to be consumed by software. It is extensively used in several anti-spam applications (SPF or DKIM).

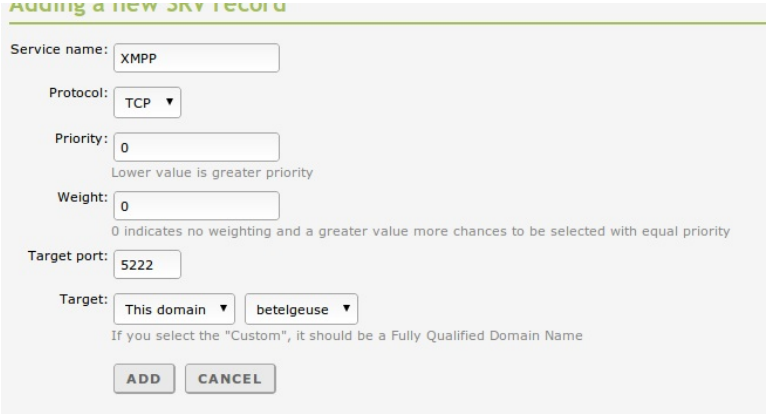


Adding a text record

To create a text record, go to the field *TXT records* of the domain. You can choose whether this record is associated with a specific hostname or the domain and its contents.

It is possible to associate more than one text record to each domain or hostname.

The **service records** provide information about the services available in your domain and which hosts are providing them. You can access the list of Service records through the field *Services* of the domain list. In each service record you can configure the *Service name* and its *Protocol*. You can identify the host that will provide the service with the fields *Target* and *Target port*. To provide better availability and/or balance the load you can define more than one record per service, in which case the fields *Priority* and *Weight* will define the server to access each time. The less priority, the more likely to be chosen. When two machines have the same priority level the weight will be used to determine which machine will receive more workload. The XMPP protocol, used mainly for instant messaging, uses these DNS records extensively. Kerberos also needs them for distributed user authentication in different services.



Adding a service record

Copyright 2004-2012 Zentyal S.L.

Time synchronization service (NTP)

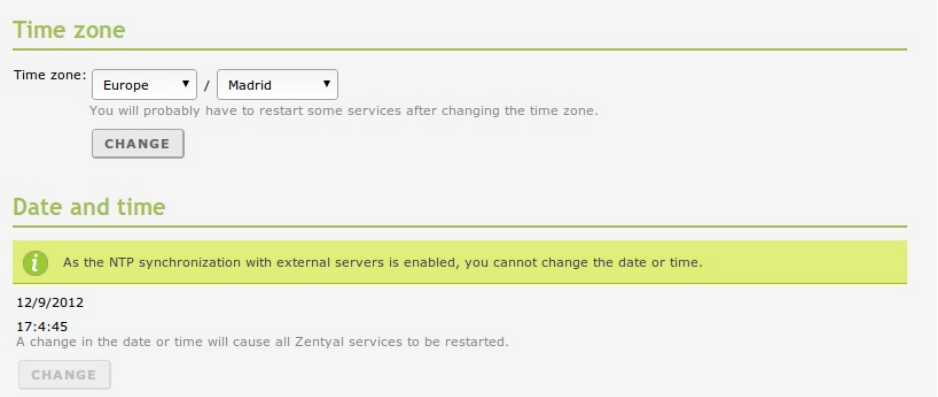
Zentyal integrates ntpd [2] as its NTP server. NTP uses UDP port 123.

[2] http://www.eecis.udel.edu/~mills/ntp/html/ntpd.html

Configuring an NTP server with Zentyal

Zentyal uses the NTP server to both synchronise its own clock and offer this service on the network, so it is important to enable it.

Once you have enabled the module, you can check in *System* ▸ *General* that it is running and that manually adjusting the time is disabled. You still need to configure your time zone.


Time zone
Time zone:
Europe
/
Madrid
You will probably have to restart some services after changing the time zone.
CHANGE
Date and time
As the NTP synchronization with external servers is enabled, you cannot change the date or time.
12/9/2012
17:4:45
A change in the date or time will cause all Zentyal services to be restarted.
CHANGE

NTP module installed and enabled

If you access to *NTP*, you can enable or disable the service, and choose the external servers that you want to synchronize to. By default, the list has already three preconfigured servers, chosen from the NTP project [3].

NTP configuration and external servers

Once Zentyal is synchronised, you can offer your clock timing using the NTP service, generally through DHCP. As always, you must not forget to check the firewall rules, as NTP is usually enabled only for internal networks.

[3] http://www.pool.ntp.org/en/

Copyright 2004-2012 Zentyal S.L.

Network configuration service (DHCP)

Zentyal uses *ISC DHCP Software* [4] to configure the DHCP service, which is the de facto standard on Linux systems. This service uses the UDP transport protocol, port 68 on the client and port 67 on the server.

[4] https://www.isc.org/software/dhcp

DHCP server configuration with Zentyal

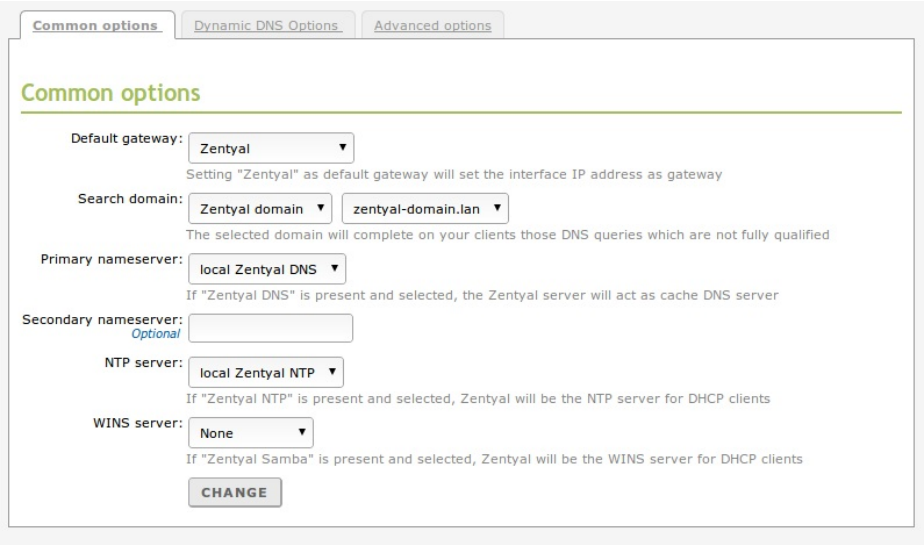
The DHCP service needs to be deployed on an interface configured with a static IP address. This interface should also be internal. From the menu *DHCP* you can find a list of interfaces on which you can offer the service.

Interfaces on which you can offer DHCP

Common options

Once you click on the configuration option of one of these interfaces,

the following form will appear:


Common options
Dynamic DNS Options
Advanced options
Common options
Default gateway:
Zentyal
Setting "Zentyal" as default gateway will set the interface IP address as gateway
Search domain:
Zentyal domain
zentyal-domain.lan
The selected domain will complete on your clients those DNS queries which are not fully qualified
Primary nameserver:
local Zentyal DNS
If "Zentyal DNS" is present and selected, the Zentyal server will act as cache DNS server
Secondary nameserver:
Optional
NTP server:
local Zentyal NTP
If "Zentyal NTP" is present and selected, Zentyal will be the NTP server for DHCP clients
WINS server:
None
If "Zentyal Samba" is present and selected, Zentyal will be the WINS server for DHCP clients
CHANGE

DHCP service configuration

The following parameters can be set in the *Common options* tab.

Default gateway:

This is the gateway that clients will use to communicate with destinations that are not on your local network, such as the Internet. Its value can be *Zentyal*, a gateway set *Network* ▸ *Routers* or a *Custom IP address*.

Search domain:

This parameter can be useful in a network where all the hosts are named under the same subdomain. Thus, when attempting to resolve a domain name unsuccessfully (for example *host*), a new attempt would be carried out by adding the search domain at the end (*host.zentyal.lan*).

Primary name server:

It specifies the DNS server that clients will use first when they have to resolve a domain name. Its value can be *Local Zentyal DNS* or the IP address of another DNS server. If you select your own Zentyal as the DNS server, make sure that the **DNS** module [5] is enabled.

Secondary name server:

DNS server to be used by clients in case primary DNS server is unavailable. Its value must be an IP address of a DNS server.

NTP server:

NTP server that clients will use to synchronise their system clock. It can be *None*, *Local Zentyal NTP* or the IP address of another NTP server. If you select your own Zentyal server as the NTP server, make sure that the **NTP** module [6] is enabled.

WINS server:

WINS server (*Windows Internet Name Service*) [7] that clients will use to resolve names on a NetBIOS network. It can be *None*, *Local Zentyal* or another *Custom*. If you select your own Zentyal server as the WINS server, make sure that the **File Sharing** module [8] is enabled.

Under these options, you can see the dynamic ranges of addresses and static allocations. For the DHCP service to work properly, you should at least have a range of addresses to distribute or static allocations; otherwise the DHCP server will **not** allocate IP addresses even when listening on all network interfaces.

Configuring DHCP ranges

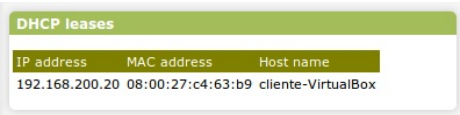
Address ranges and static addresses available for assignment from a certain interface are determined by the static address assigned to that interface. Any available IP address of the subnet can be used in ranges or static allocations.

In order to add a range in the *Range* section you have to introduce a *name* to identify the range and the values you want to assign within the range listed above.

You can perform static assignment of IP addresses to specific physical

addresses in the *Fixed addresses* section. To fill this section you need an object which members are pairs of host IP addresses (/32) and MAC addresses. You can create this object from *Network* ▸ *Objects* or directly in the quick menu offered in the DHCP interface. An address assigned in this way can not be part of any range. You can add an optional *Description* for the allocation as well.

You can se DHCP clients with dynamic allocations (static allocations will not be shown) thanks to a widget that will appear in the Dashboard:

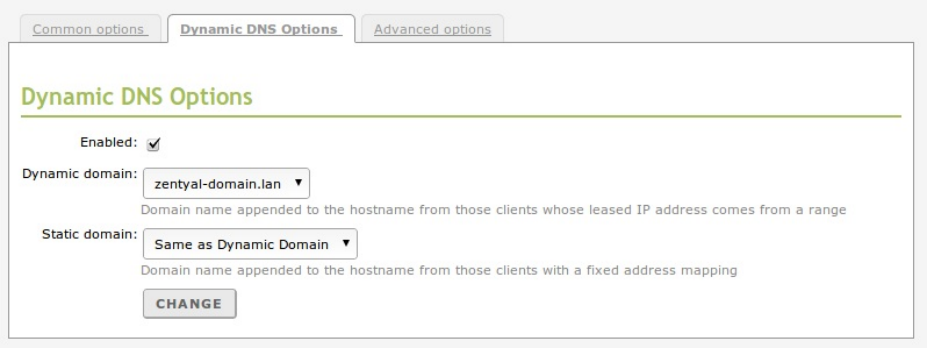


Client with dynamic allocation enabled

[5] See *Domain Name System (DNS)* section for details.
[6] See *Time synchronization service (NTP)* section for details.
[7] http://en.wikipedia.org/wiki/Windows_Internet_Name_Service
[8] See *File sharing and authentication service* section for details.

Dynamic DNS options

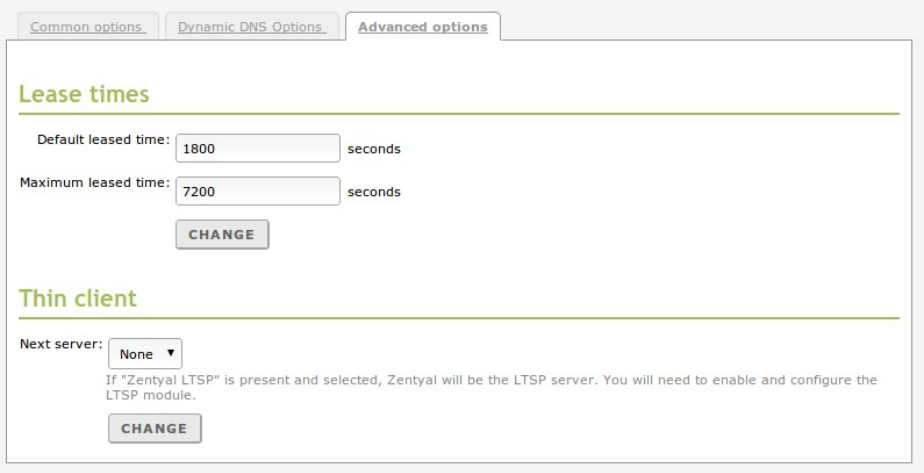
The dynamic DNS options will allow to assign domain names to DHCP clients through the integration of DHCP and DNS modules. Thanks to this it is easier to recognize machines located in the network: they can be recognized by an unique domain name instead of an IP address that might change.


Common options
Dynamic DNS Options
Advanced options
Dynamic DNS Options
Enabled:
Dynamic domain:
zentyal-domain.lan
Domain name appended to the hostname from those clients whose leased IP address comes from a range
Static domain:
Same as Dynamic Domain
Domain name appended to the hostname from those clients with a fixed address mapping
CHANGE

Configuration of dynamic DNS updates

To use this option, you must go to the tab "Dynamic DNS options" and to enable the feature, the DNS module must be enabled as well. You must have both Dynamic domain and Static domain: both will be added automatically to the DNS configuration. The dynamic domain will host the names of those machines which IP addresses belong to the range and the name associated is the one sent by the DHCP client, usually the host name. If none is sent, the pattern *dhcp-<offered-IP-address>.<dynamic-domain>* will be used. If there are any conflicts with a static allocation, the established static address will be overwritten manually. As to the static domain, the host name will follow this pattern: *<name>.<static-domain>*. The *name* will be the one registered in the object used in the static allocation.

Advanced options



Advanced DHCP options

The dynamic address allocation has a time limit. After expiry of that time a renewal must be requested (configurable in the *Advanced options* tab). This time varies from 1800 seconds to 7200. This limitation also applies to the static allocation.

Zentyal supports remote boot for thin clients through DHCP. In the *Advanced options* tab you can configure a thin client that will be published through DHCP. If Zentyal is not used as a thin client server, in *Host* select the remote host and in *File route* select the route to find the image within the server.

In case Zentyal is used as a thin client server, choose image *Architecture*. You can also choose if you want to use thin or fat client [10]. To do this, you must have created the mentioned image previously, as well as have carried out the rest of the configurations that will be explained in the *Thin client service (LTSP)*.

[10] Detailed information regarding the differences between thin and fat clients:
https://help.ubuntu.com/community/UbuntuLTSP/FatClients

Copyright 2004-2012 Zentyal S.L.

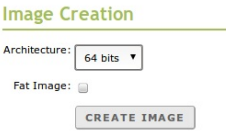
Thin client service (LTSP)

Configuration of a thin client server with Zentyal

Creation of thin client images

To start with, you have to create the images that will be sent through the network to your thin clients. In the context of thin clients you must take into consideration that the applications will be run on the operating system of the server, expect for the *local applications* or fat clients that will be mentioned later in this chapter. Therefore you must install a desktop environment and all the other applications that you wish to use on the thin clients.

Once the necessary applications/environments are installed, you can start building the image by going to *Thin clients* tab *Create thin client images*. Here you choose the hardware architecture compatible with the client hardware, if you wish the clients to act as thin or fat clients [6] and finally click on *Create image*.

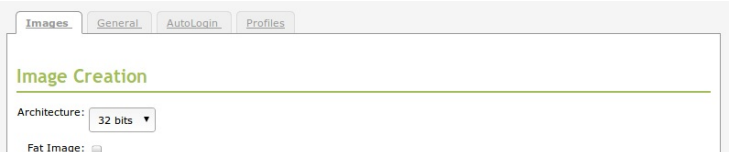


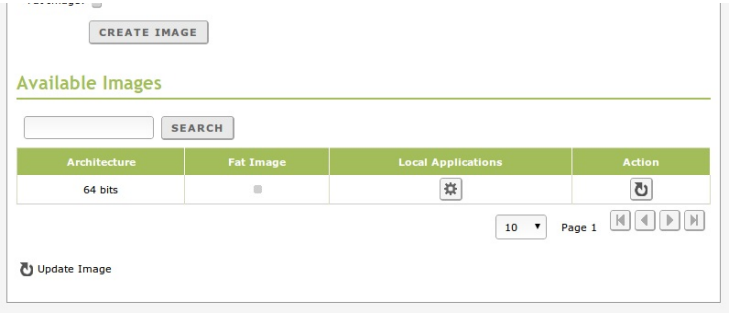
Creating thin client image

After this you are informed that Zentyal will proceed with the creation of the image. You can follow the progress through a *widget* available in the *Dashboard*.

Widget with the status of the new image

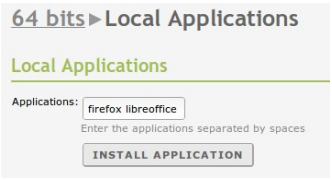
Once the process has finished, you can see the list of available images by returning to the *Thin clients* tab *Create thin client images*.





List of available images

As you can see, it is possible to update the image. This will allow to update the core of the operating system or the *local applications* within the image. Through this menu you can also configure those applications that will be considered as **local applications**.



Applications that will be run locally

The local applications will allow to run some applications in the thin client hardware. This can be useful option if the applications are creating too much load for the server or network traffic. As you can see in the following section, to make this work, it is necessary to enable the *Local applications* in the *General configuration* tab.

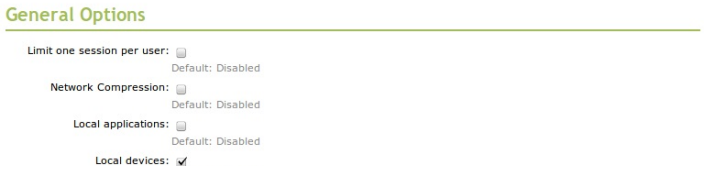
[6] https://help.ubuntu.com/community/UbuntuLTSP/FatClients

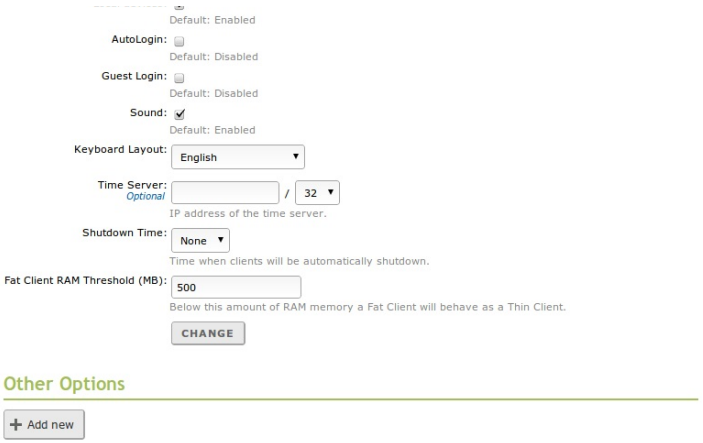
In the context of LTSP you can find a series of differences between thin clients and fat clients. The most important differences are:

- Fat clients use their own RAM and CPU to run processes.
- In fat clients the *home* directories will be mounted locally, in thin clients they are accessed remotely.
- In fat clients the desktop environment is installed and run locally.

General server configuration

Once you have the thin client image(s) prepared, you have to carry out the general server configuration.





General configuration of thin client server

Limit to one session per user:

Prevent the same user having multiple open sessions simultaneously.

Network compression:

Send the network traffic compressed, useful to reduce the network load at the expense of higher computing load.

Local applications:

Allow applications that will be run on thin clients.

Local devices:

Allow the use of local appliances, such as USB memories, from thin clients.

AutoLogin:

As you will see in the section *AutoLogin*, this option will allow login depending on the network MAC in the thin client.

Guest Login:

Here you can decide whether limited login will be possible without a personal account.

Sound:

The thin client will be able to reproduce sound if this option is enabled.

Keyboard layout:

Mapping between keys and characters to apply.

Time server:

Server to update the time in the clients, by default it will be the same as used for the images.

Shutdown time:

In some cases you might want to switch off at a specific time a room of thin clients, this option allows you to specify the time

FAT Client RAM Threshold (MB):

The clients that were provided a fat client image, but do not reach this RAM threshold will behave like thin clients.

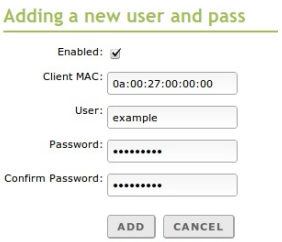
The *LTSP* server associated with the thin client module of Zentyal

The LTSP server associated with the thin client module of Zentyal counts on many more advanced configuration options. In case you want to use one of the options not mentioned here, the interface gives you the option to add it as a name-value pair in the lower part of the form *Other options* [7].

[7] http://manpages.ubuntu.com/manpages/precise/man5/lts.conf.5.html

Configuration of automatic login

If this option has been enable, as mentioned in the previous section, it is possible for a thin client to login directly depending on its MAC address.

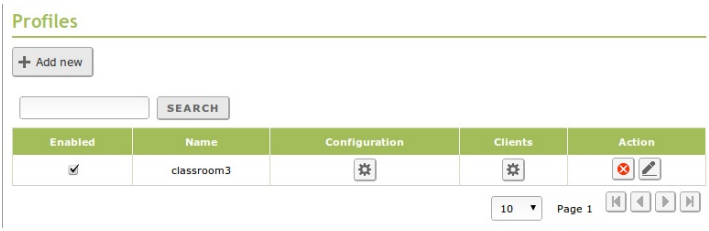


Automatic login

This configuration might be useful if, as usual in LTSP, the computers are used randomly by different people. For example, if you have a computer in a computer class that any person can use, you can avoid management of personal passwords.

Profile configuration

You might want to deploy a infrastructure where from a central server you can serve different images and/or configurations, depending on the network objective that you wish to serve. To do this, Zentyal offers the possibility to configure *profiles*.



Configuration profiles

Each one of these profiles will have some associated clients, that will be defined through the Zentyal objects *High-level Zentyal abstractions*.

Profile will be applied on these clients

Through the configuration form associated with the profile (similar to the general configuration), you can decide whether for each one of the parameters you want to apply the values defined in the general configuration or other specific values.

Download and run thin client

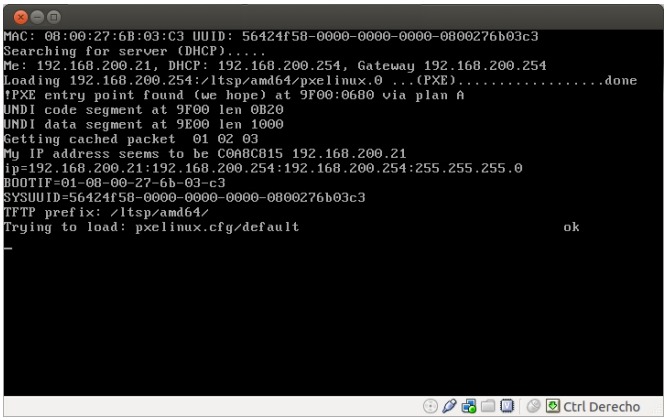
Once the images are created and the server is configured, you can configure the clients to download and run them. In the first place you need to make sure that the DHCP module will notify when the images are available. This can be done with Zentyal's own DHCP module.

Thin client
Next server:
Zentyal LTSP
If "Zentyal LTSP" is present and selected, Zentyal will be the LTSP server. You will need to enable and configure the LTSP module.
Host:
Optional
Thin Client server as seen by the clients.
Architecture:
64 bits
Architecture of the LTSP clients. The LTSP image for that architecture must exist in order to boot the clients.
Fat Client:
Whether the clients are fat clients or not.
CHANGE

DHCP configuration - Thin client

Once the DHCP is configured, you will need to make sure that you clients have *Network boot* as the first boot option, generally this is configured through the BIOS of the computer.

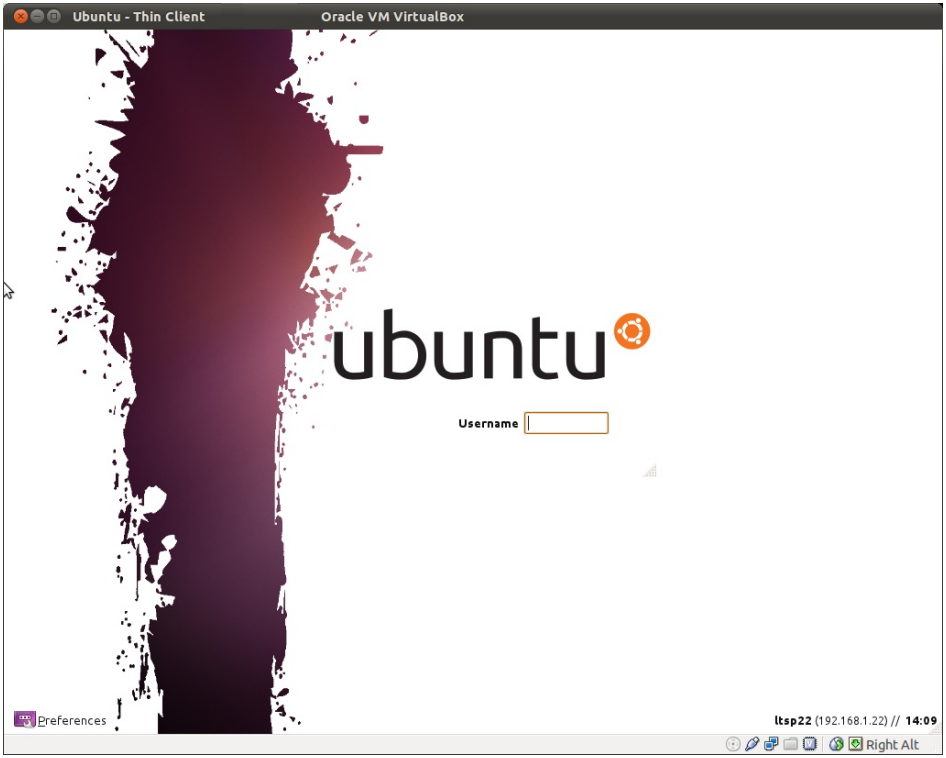
To boot over the network, your DHCP server will redirect it to the TFTP server that has the image:


MAC: 08:00:27:6B:03:C3 UUID: 56424f58-0000-0000-0000-0800276b03c3
Searching for server (DHCP)....
Me: 192.168.200.21, DHCP: 192.168.200.254, Gateway 192.168.200.254
Loading 192.168.200.254:/ltsp/amd64/pxelinux.0 ...(PXE).....done
!PXE entry point found (we hope) at 9F00:0680 via plan A
UNDI code segment at 9F00 len 0B20
UNDI data segment at 9E00 len 1000
Getting cached packet 01 02 03
My IP address seems to be C0A8C815 192.168.200.21
ip=192.168.200.21:192.168.200.254:192.168.200.254:255.255.255.0
BOOTIF=01-08-00-27-6b-03-c3
SYSUUID=56424f58-0000-0000-0000-0800276b03c3
TFTP prefix: /ltsp/amd64/
Trying to load: pxelinux.cfg/default ok
Ctrl Derecho

Client booting an image over the network

When the load finishes, you have your thin client running:

When the load finishes, you have your thin client running:



Thin client running

Obviously the users that can login in the thin client will be configured through Zentyal's *Directory Service (LDAP)* module.

Copyright 2004-2012 Zentyal S.L.

Certification authority (CA)

Zentyal uses **OpenSSL** [4] for the management of the Certification Authority and the life cycle of the issued certificates issued.

[4] http://www.openssl.org/

Certification Authority configuration with Zentyal

In Zentyal, the **Certification Authority** module is self-managed, which means that it does not need to be enabled in *Module status*. However, you have to initialize the CA to make the functionality of the module available.

Go to *Certification Authority* ‣ *General* and you will find the form to create the CA. You are required to fill in the *Organization Name* and *Days to expire* fields. Optionally, it is possible to specify the *Country code* (a two-letter acronym following the ISO-3166-1 standard [5]), *City* and *State*.

Create the CA certificate

When setting the expiration date you have to take into account that at the moment of expiration all certificates issued by this CA will be

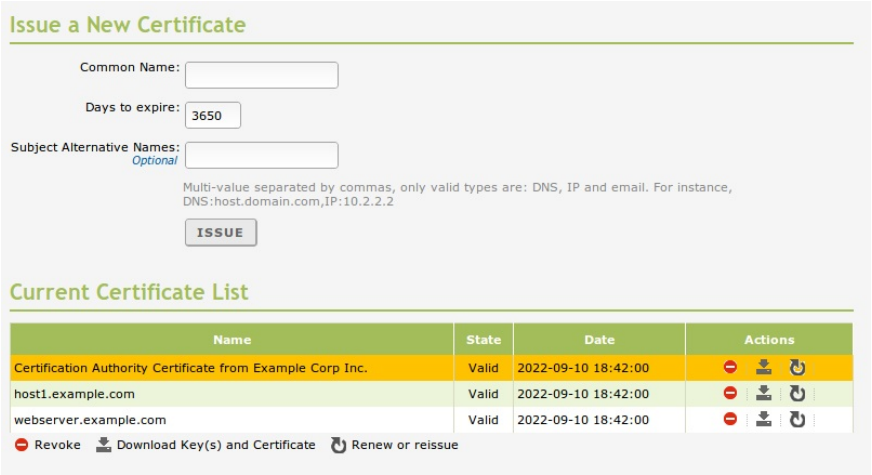
revoked, stopping all services depending on those certificates.

Once the CA has been initialised, you will be able to issue certificates. The required data are the *Common Name* of the certificate and the *Days to expire*. This last field is limited by the fact that no certificate can be valid for a longer time than the CA. In case you are using the certificate for a service such as a web server or mail server, the *Common Name* of the certificate should match the domain name of that server. For example, if you are using the domain name *zentyal.home.lan* to access the web administrative interface in Zentyal, you will need a certificate with the same *Common Name*. In case you are setting a user certificate, the *Common Name* will usually be the user's email address.

Optionally, you could set *Subject Alternative Names* [6] for the certificate. These are useful when setting common names to a certificate: a domain name or an IP address for a HTTP virtual host or an email address when signing email messages.

Once the certificate is issued, it will appear in the list of certificates and it will be available for the administrator and for the rest of modules. Through the certificate list you can perform several actions on the certificates:

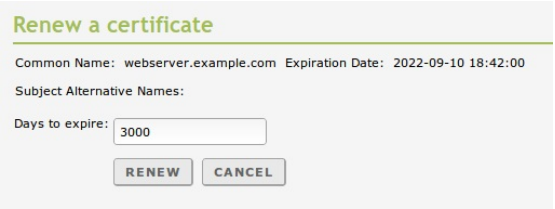
- Download the public key, private key and the certificate.
- Renew the certificate.
- Revoke the certificate.
- Reissue a previously revoked or expired certificate.



Certificate list page

The package with the keys contains also a PKCS12 file with the private key and the certificate and it can be installed directly into other programs such as web browsers, mail clients, etc.

If you renew a certificate, the current certificate will be revoked and a new one with the new expiration date will be issued. And if you renew the CA, all certificates will be renewed with the new CA trying to keep the old expiration date. If this is not possible because it is after the date of expiry of the CA, then the date of expiration is set as the one of the CA.



Renew a certificate

If you revoke a certificate you will not be able to use it anymore as this action is permanent and it can not be undone. Optionally, you can select the reason of the certificate revocation:

- *unspecified*: reason non specified,
- *keyCompromise*: the private key has been compromised,
- *CACompromise*: the private key for the certification authority has been compromised,
- *affilliationChanged*: the issued certificate has changed its affiliation to another certification authority from other organization,
- *superseded*: the certificate has been renewed and it is now replaced by a new one,
- *cessationOfOperation*: the certification authority has ceased its operations,
- *certificateHold*: certified suspended,
- *removeFromCRL*: currently unimplemented, it provides delta CRLs support, that is, lists of certificates whose revoked status has changed.

Revoke a certificate

When a certificate expires all the modules are notified. The expiration date of each certificate is automatically checked once a day and every time you access the certificate list page.

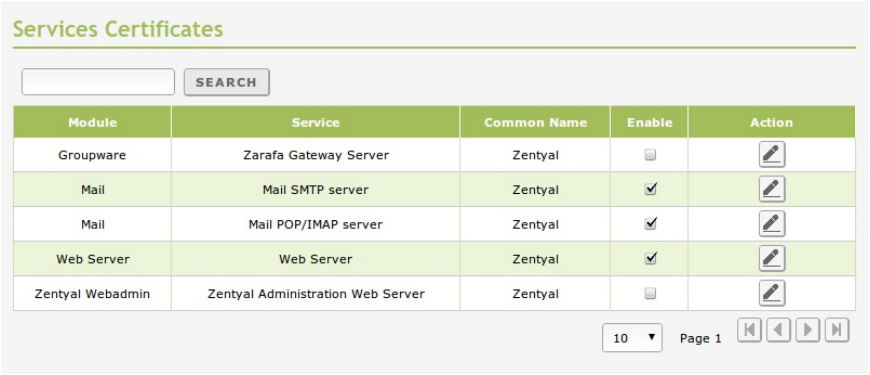
[5] http://en.wikipedia.org/wiki/ISO_3166-1

[6] For more information about *subject alternative names*, visit http://www.openssl.org/docs/apps/x509v3_config.html#Subject_Alternative_Name

Services Certificates

On *Certification Authority ▸ Services Certificates* you can find the list of Zentyal modules using certificates for their operation. Each module generates its own self-signed certificates, but you can replace them with others issued by your CA.

You can generate a certificate for each service by defining its *Common Name*. If a previous certificate with the name does not exist, the CA will create it automatically.



Services Certificates

Once enabled, you need to restart the service to force the module to use the new certificate. This also applies if you renew a certificate for a module.

As mentioned before, to use the secure version of multiple protocols (web, email, etc.) it is important that the name that appears in the "Common name" of the certificate matches with the name requested by

the client. For example, if the *Common name* of your web certificate is *host1.example.com* and the client types in *https://www.example.com*, the browser will show a security alert and the certificate is not considered valid.

Copyright 2004-2012 Zentyal S.L.

Virtual private network (VPN) service with OpenVPN

Zentyal integrates OpenVPN [2] PPTP and IPsec to configure and manage virtual private networks. In this section you will see how to configure OpenVPN, the default VPN protocol in Zentyal. In the following section you will find out how to configure PPTP and IPsec.

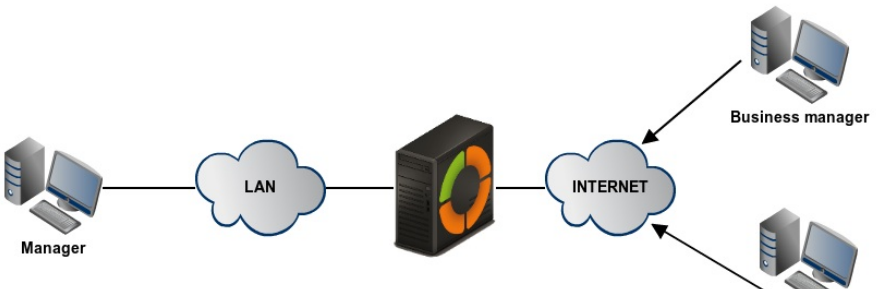
OpenVPN has the following advantages:

- Authentication using public key infrastructure.
- SSL-based encryption technology.
- Clients available for Windows, Mac OS and Linux.
- Easier to install, configure and maintain than IPSec, another open source VPN alternative.
- Allows to use network applications transparently.

[2] http://openvpn.net/

Configuration of a OpenVPN server with Zentyal

Zentyal can be configured to support remote clients (sometimes known as road warriors). This means a Zentyal server acting as a gateway and VPN server, with multiple local area networks (LAN) behind it, allows external clients (the *road warriors*) to connect to the local network via the VPN service.



Zentyal and remote VPN clients

The goal is to connect the data server with other 2 remote clients (sales person and CEO) and also the remote clients to each other.

First, you need to create a **Certification Authority** and individual certificates for the two remote clients. You can do this through *Certification Authority* ▸ *General*. Note that you also need a certificate for the VPN server. However, Zentyal will create this certificate automatically when you create a new VPN server. In this scenario, Zentyal acts as a **Certification Authority**.

Server certificate (blue underline) and client certificate (black underline)

Once you have the certificates, then configure the Zentyal VPN server by selecting *Create a new server*. The only value you need to enter to create a new server is the name. Zentyal ensures the task of creating a VPN server is easy and it sets the necessary values automatically.

New VPN server created

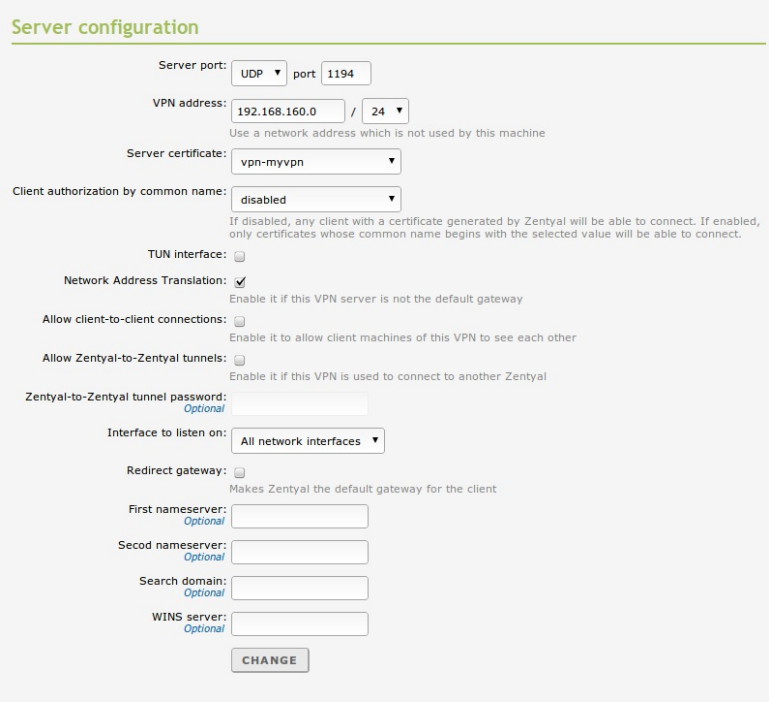
The following configuration parameters are added automatically and can be changed if necessary: *port/protocol*, *certificate* (Zentyal will create one automatically using the VPN server name) and *network address*. The VPN network addresses are assigned both to the server and the clients. If you need to change the *network address* you must make sure that there is no conflict with a local network. In addition, you will automatically be notified of local network detail, i.e. the

networks connected directly to the network interfaces of the host, through the private network.

As you can see, the VPN server will be listening on all external interfaces. Therefore, you must set at least one of your interfaces as external at *Network ▸ Interfaces*. In this scenario only two interfaces are required, one internal for LAN and one external for Internet.

If you want the VPN clients to connect between themselves by using their VPN addresses, you must enable the option *Allow connections among clients*.

In most of the cases you can leave the rest of the configuration options with their default values.



VPN server configuration

In case more advanced configuration is necessary:

VPN address:

Indicates the virtual subnet where the VPN server will be located and the clients it has. You must take care that this network does not overlap with any other and for the purposes of firewall, it is an internal network. By default *192.168.160.1/24*, the clients will get addresses *.2*,*.3*, etc.

Server certificate:

Certificate that will show the server to its clients. The Zentyal CA issues by default a certificate for the server, with the name vpn-<yourvpnname>. Unless you want to import an external certificate, usually you maintain this configuration.

Authorize the client by the common name:

Requires that the *common name* of the client certificate will start with the selected string of characters to authorize the connection.

TUN interface:

By default a *TAP* type interface is used, more similar to a *bridge* of Layer 2. You can also use a *TUN* type interface more similar to a IP node of Layer 3.

Network Address Translation (NAT):

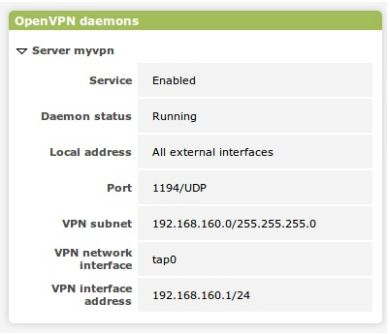
It is recommended to enable this translation if the Zentyal server that accepts the VPN connections is not a default gateway of the internal networks to which you can access from the VPN. Like this the clients of these internal networks respond to Zentyal's VPN instead of the gateway. If Zentyal server is both the VPN server and the gateway (most common case), this option is indifferent.

Redirect gateway:

If this option is not checked, the external client will access through the VPN to the established networks, but will use his/her local connection to access to Internet and/or rest of the reachable networks. By checking this option you can achieve that all the traffic of the client will go through the VPN.

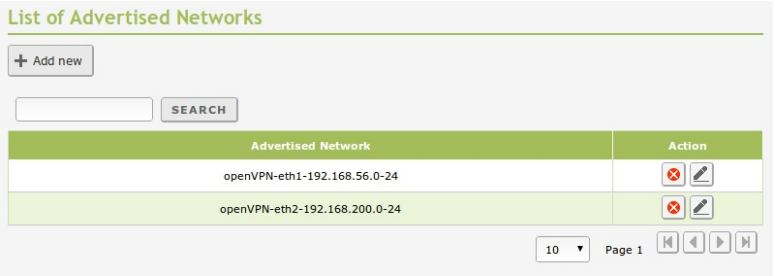
The VPN can also indicate name servers, search domain and WINS servers to overwrite those of the client. This is specially useful in the case you have redirected the gateway.

After having created the VPN server, you must enable the service and save the changes. Later you must check in *Dashboard* that the VPN server is running.



Widget of the VPN server

After this, you must advertise networks, i.e. routes between the VPN networks and between other networks known by your server. These networks will be accessible by authorised VPN clients. To do this, you have to enable the objects you have defined, see *High-level Zentyal abstractions*, in the most common case, all internal networks. You can configure the advertised networks for this VPN server through the interface of *Advertised networks*.



Advertised networks of your VPN server

Once you have done this, it is time to configure the clients. The easiest way to configure a VPN client is by using the Zentyal *bundles* - installation packages that include the VPN configuration file specific to each user and optionally, an installation program. These are available in the table at *VPN ‣ Servers*, by clicking the icon in the column *Download client bundle*. You can create *bundles* for Windows, Mac OS and Linux clients. When you create a *bundle*, select those certificates that will be used by the clients and set the external IP addresses to which the VPN clients must connect.

As you can see the image below, you have one main VPN server and up to two secondary servers, depending on the *Connection strategy* you will try establishing connection in order or trying a random one.

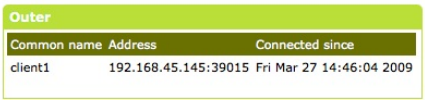
Moreover, if the selected system is Windows, you can also add an OpenVPN installer. The Zentyal administrator will download the configuration *bundles* to the clients using the most appropriate method.

Download client bundle

A *bundle* includes the configuration file and the necessary files to start a VPN connection.

You now have access to the data server from both remote clients. If you want to use the local Zentyal DNS service through the private network, you need to configure these clients to use Zentyal as name server. Otherwise, it will not be possible to access services by the hosts in the LAN by name, but only by IP address. Also, to browse shared files from the VPN [3] you must explicitly allow the broadcast of traffic from the Samba server.

You can see the users currently connected to the VPN service in the Zentyal *Dashboard*. You need to add this *widget* from *Configure widgets*, located in the upper part of the *Dashboard*.



Widget with connected clients

[3] For additional information about file sharing go to section *File sharing and authentication service*

Copyright 2004-2012 Zentyal S.L.

Virtual private network (VPN) service with PPTP

Zentyal integrates pptpd [2] as its PPTP server. This service uses the port 1723 of the TCP protocol and the GRE encapsulation protocol.

[2] http://poptop.sourceforge.net/

Configuring a PPTP server in Zentyal

To configure your PPTP server in Zentyal go to *VPN* ▸ *PPTP*. In the *General configuration* tab define the subnet used for the VPN. This subnet has to be different to any other internal network you are using in your local network or another VPN. You can also define the *Primary Nameserver* and *Secondary Nameserver*. In the same way you can configure the *Primary WINS* and *Secondary WINS* servers.

General configuration

Given the limitations of the PPTP server, it is not currently possible to integrate the LDAP users, managed through *Users and Groups*, so it will be in the tab *PPTP Users* where you will define the list of users and its associated passwords that will be able to connect to the VPN

PPTP server. Additionally, you can statically assign the same IP address to a user inside the VPN subnet, using the configuration field *IP Address*.

PPTP Users

As usual, before being able to connect to your PPTP server, you have to check that the current rules of the firewall allow the connection to the PPTP server, which includes the 1723/TCP port and the GRE protocol.

Copyright 2004-2012 Zentyal S.L.

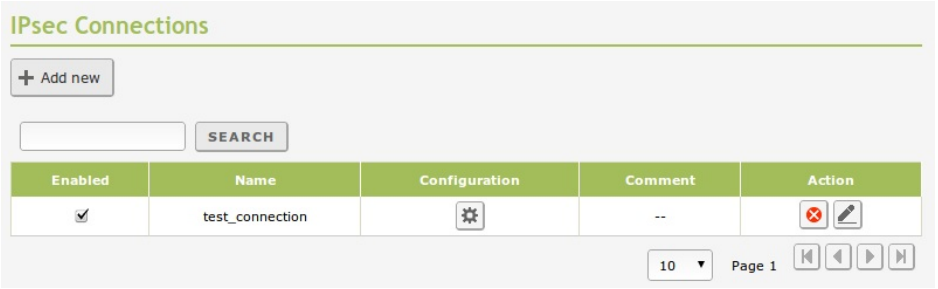
Virtual Private Network (VPN) Service with IPsec

Zentyal integrates OpenSwan [2] as its IPsec solution. This service uses the ports 500 and 4500 of UDP and the ESP protocol.

[2] http://www.openswan.org/

Configuring an IPsec tunnel in Zentyal

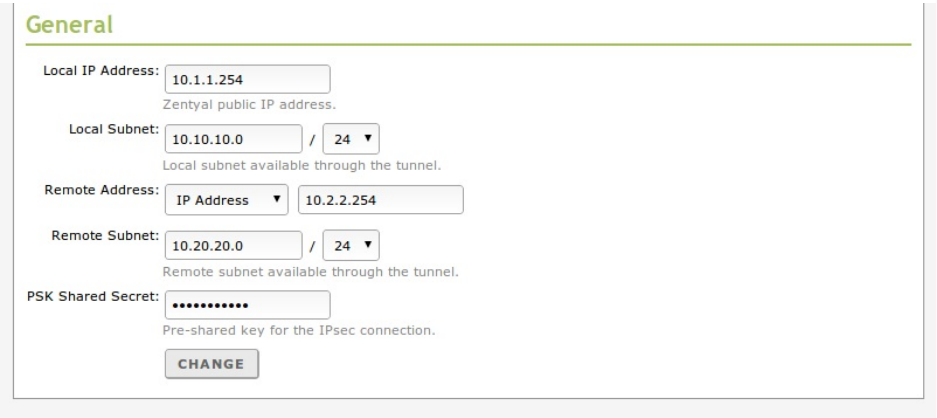
To configure IPsec in Zentyal go to *VPN* ▸ *IPsec*. Here you can define all the tunnels and IPsec connections you need. You can enable or disable each one of them and add an explanatory text.



IPsec connections

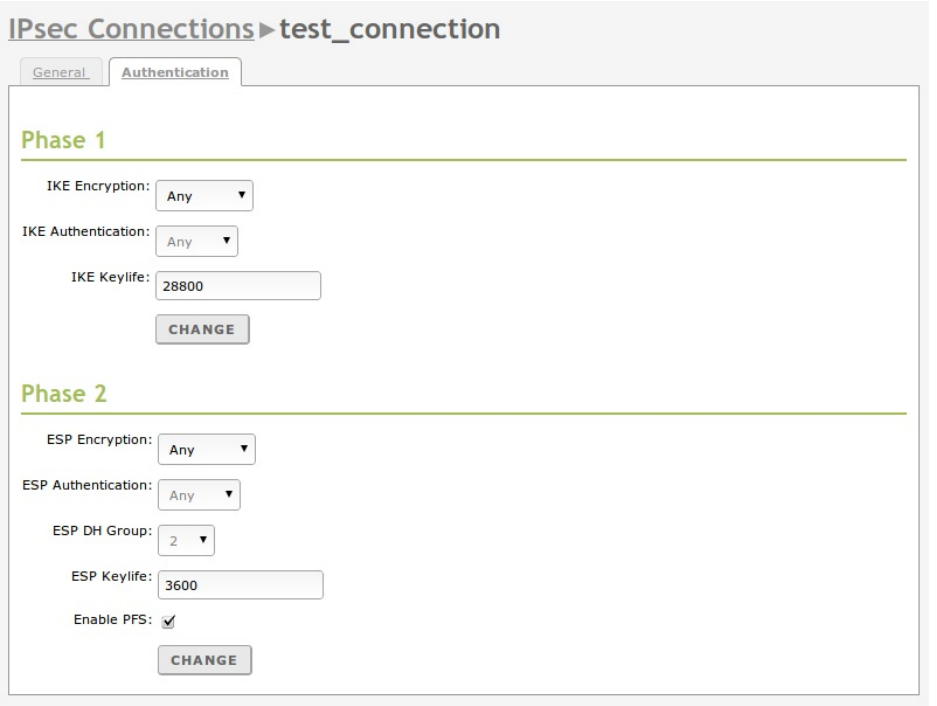
Inside *Configuration*, and the *General* tab you will define the Zentyal's IP address that you will use in each connection to access the external subnet, the local subnet behind Zentyal that will be accessible through the VPN tunnel, the remote IP address you will contact in the other end of the tunnel and the local subnetwork you will have available in the other end. If you want to configure a tunnel between two networks using IPsec, both ends must have a static IP address.

Currently Zentyal supports PSK authentication only (preshared key), which you can configure under *PSK preshared key*.



General configuration

In the *Authentication* tab you will configure the specific parameters of the tunnel authentication. This parameters determine the behaviour of the IPsec protocol and have to be identical in both ends of the tunnel. To learn more about the meaning of each one of the options, check IPsec specific documentation.



Authentication configuration

Copyright 2004-2012 Zentyal S.L.

Virtualization Manager

Zentyal offers easy management of virtual machines by integrating the KVM [1] solution.

[1] http://en.wikipedia.org/wiki/Kernel-based_Virtual_Machine

Creating virtual machines with Zentyal

Through the *Virtual Machines* menu you can access the list of currently available machines, as well as add new ones or delete the existing ones. You also have other maintenance options that will be described in detail in the next section.

When you create a machine, you have to click in *Add new* and then fill the following parameters:

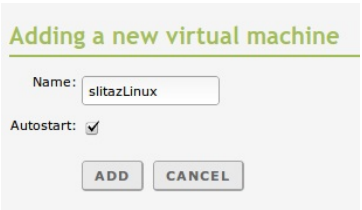
Name

> Just for identification purposes, it will also be used to pick the file system path where you will store the data associated with this machine, but essentially, you can enter any alphanumeric label.

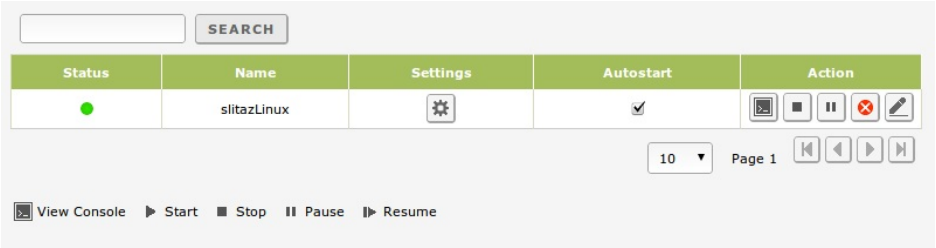
and decide whether you want to:

Autostart

> If this option is enabled, Zentyal will be in charge of starting or stopping the machine along with the rest of the services, otherwise Zentyal will just create the machine the first time you configure it and save changes. The system administrator will be in charge of performing these actions manually when he/she considers necessary.



After this, you have a configuration row associated with your new machine.

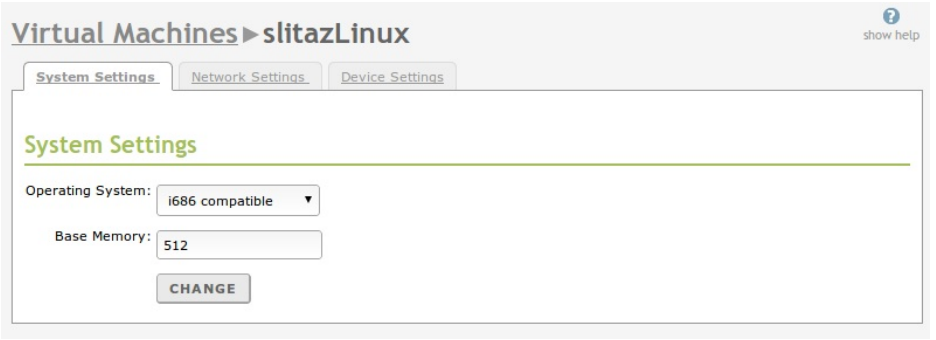


Virtual machine registered in the table

The next step will be configuring your new virtual machine, through the *Settings* column, where you will find the following tabs:

System Settings

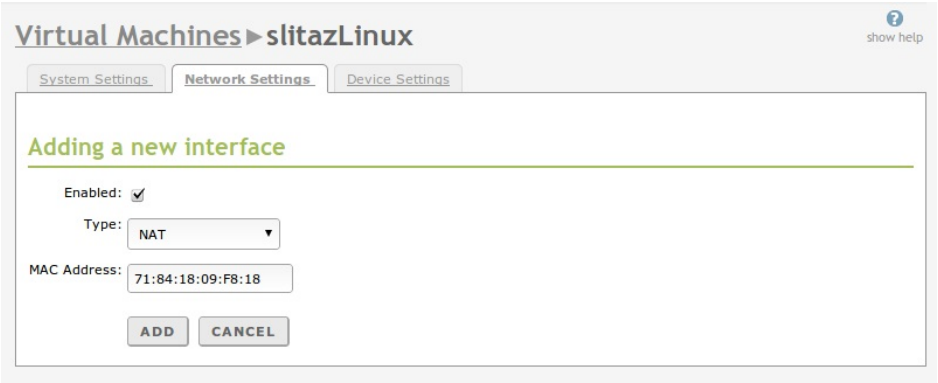
It allows you to define the architecture (32 or 64 bits). You can also define the size of the RAM memory allocated for this machine in megabytes. By default this value is 512, or half the available memory if you have less than 1GB in the real host.



System configuration for the virtual machine

Network Settings

It contains the list of network interfaces of the virtual machine, which can be configured as NAT (only Internet access), in bridged mode with one of the host system interfaces or forming an isolated internal network, which name you have to define, so other virtual machines will be able to connect. If you uncheck the *Enabled* checkbox, you can temporally disable any of the configured network interfaces. As you can see below, it is possible to modify also the MAC address associated to this interface.



VM network settings

Device Settings

It contains the list of storage drives associated with the machine. You can associate CDs or DVDs (providing the path to an ISO image), and also hard drives. For the hard drives, you can also provide a image file of either KVM or VirtualBox, or just specify the size in megabytes and an identifier name and Zentyal will create the new empty disk. By unchecking the checkbox *Enabled*, you can temporally disconnect any of the drives without deleting them.

Device settings

Virtual machine maintenance

In the *Dashboard* you have a widget that contains the list of virtual machines and their current state (running or not), and a button that allows you to *Stop* or *Start* them if you want to.

Widget in your Dashboard

In the *Virtual Machines* section you can see, from left to right, the following actions you can execute over a machine:

Highlighting the action buttons and status indicator

Besides the delete and edit buttons, you can carry out the following actions:

View Console

It will open a pop-up window where you can access to the terminal of the virtual machine, using the VNC protocol.

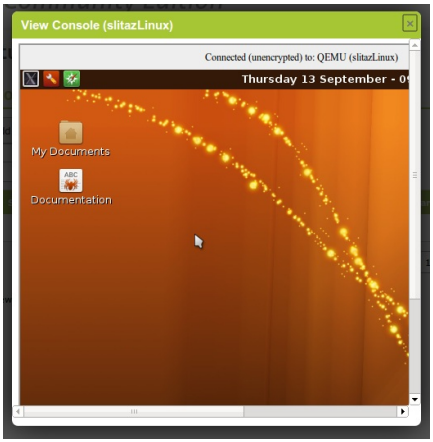
Start/Stop

It allows you to start or stop the machine, depending on its current state. In case the machine is in 'Pause' state, the 'start button' will resume execution.

Pause/Continue

From here you can pause the execution of the machine while it is running, without losing the running state. Once the machine is pause, you can click the same button to resume execution.

At the top left you can also see an indicator that be either red, yellow or green depending whether the machine is stopped, paused or running.



Example window showing the console window of a machine

Copyright 2004-2012 Zentyal S.L.

Zentyal Gateway

This chapter focuses on the functionality of Zentyal as a *gateway*. Offering more reliable and secure networks, bandwidth management and clear definition of connection and content policies.

One of the main chapters is dedicated to the firewall module, which allows you to define connection management rules for both the incoming and outgoing traffic. To simplify the firewall configuration, you will categorize the types of traffic depending on their origin and destination, and you will also use your defined objects and services.

You can define the traffic balancing of your gateways when accessing resources on the Internet, configuring the protocols associated with each gateway, wan-failover safety politics and bandwidth restrictions for some types of traffic, like P2P.

Using RADIUS, you can authenticate the users in your network, is specially useful if you want to avoid the security problems associated with symmetric password on wireless networks.

Another needed service in most of the deployments is the HTTP Proxy. This service allows you to speed up your Internet connection, storing a web cache and establishing advanced access politics.

The Captive Portal with bandwidth monitoring allows you to give access to a set of users, redirecting all the web traffic to your registration webpage. It sports real-time reports of connected users and their consumed traffic.

Thanks to the IDS module you can stablish heuristics to automatically detect a diverse group of security threats, in both internal and external networks.

Copyright 2004-2012 Zentyal S.L.

Firewall

Zentyal uses the Linux kernel subsystem called Netfilter [2] in the firewall module. Functionality includes filtering, package marking and connection redirection capabilities.

[2] http://www.netfilter.org/

Firewall configuration with Zentyal

Zentyal's security model is based on delivering the maximum possible security with the default configuration, trying at the same time to minimise the effort when adding a new service.

When Zentyal is configured as a firewall, it is normally installed between the internal network and the *router* connected to the Internet. The network interface which connects the host with the *router* has to be marked as *External* in *Network -> Interfaces*, therefore the firewall can establish stricter policies for connections initiated outside your network.

External interface

The default policy for external interfaces is to deny any new connections. On the other hand, for internal interfaces, Zentyal denies all the connection attempts, except the ones that are targeted to services defined by the installed modules. The modules add rules to the firewall to allow these connections. These rules can be modified later by the system administrator. An exception to this are the connections to the LDAP server, which add a rule but it is configured to deny the connection for security reasons. The default configuration for

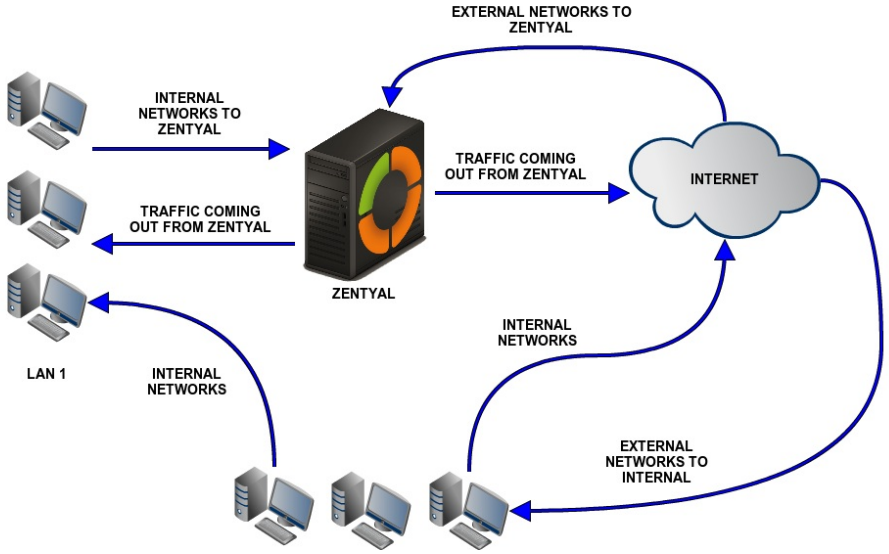
connections to hosts outside the network and connections from the server itself is allow all.

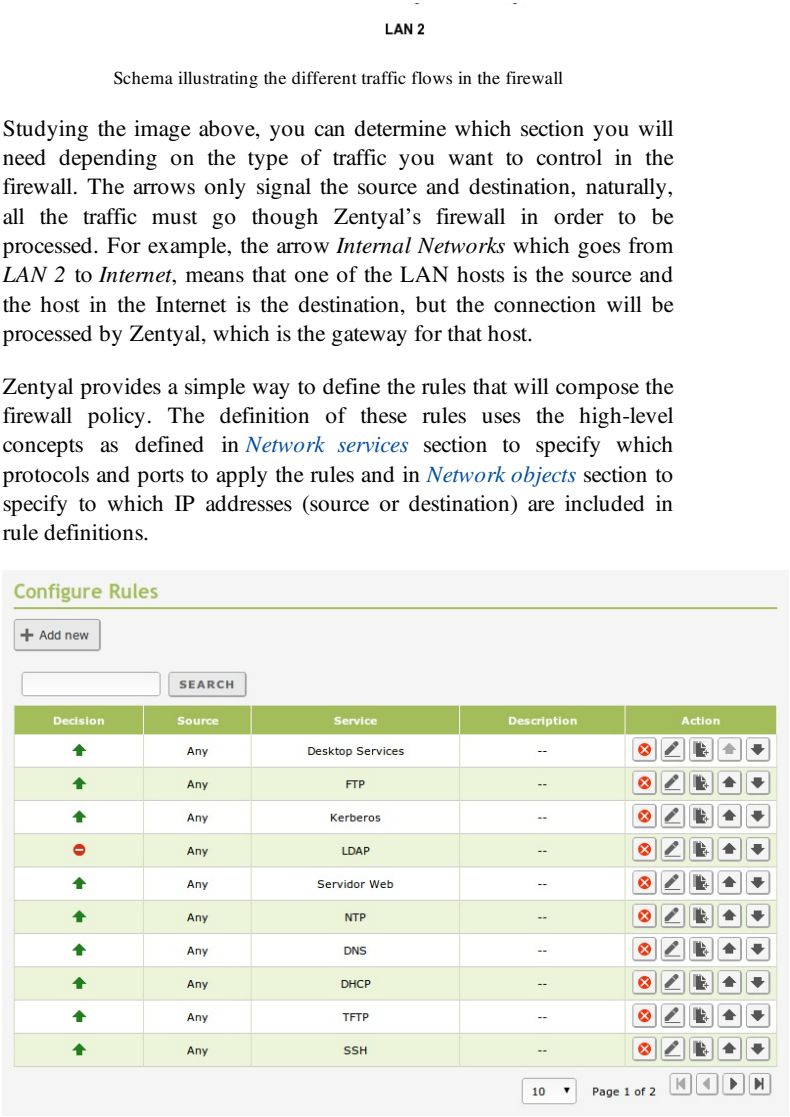
Definition of firewall policies can be made from: *Firewall ▸ Packet filtering*.

Five different sections are available for configuration depending on the work flow of the traffic you are addressing:

- *Traffic from internal networks to Zentyal* (example: allow access to the file server from the local network).
- *Traffic between internal networks and from internal networks to the Internet* (example: restrict access to Internet or to specific addresses to some internal clients and restrict communication between internal networks)
- *Traffic from Zentyal to external networks* (example: allow to download files using HTTP from the server itself).
- *Traffic from external networks to Zentyal* (example: allow the mail server to receive messages from the Internet).
- *Traffic from external networks to internal networks* (example: allow access to a internal server from the Internet).

You have to take into account that the last two types of rules could compromise the security of Zentyal and the network, so you must be very careful when modifying them.





Schema illustrating the different traffic flows in the firewall

Studying the image above, you can determine which section you will need depending on the type of traffic you want to control in the firewall. The arrows only signal the source and destination, naturally, all the traffic must go though Zentyal's firewall in order to be processed. For example, the arrow *Internal Networks* which goes from *LAN 2* to *Internet*, means that one of the LAN hosts is the source and the host in the Internet is the destination, but the connection will be processed by Zentyal, which is the gateway for that host.

Zentyal provides a simple way to define the rules that will compose the firewall policy. The definition of these rules uses the high-level concepts as defined in *Network services* section to specify which protocols and ports to apply the rules and in *Network objects* section to specify to which IP addresses (source or destination) are included in rule definitions.

List of package filtering rules from internal networks to Zentyal

Normally, each rule has a *Source* and a *Destination* which can be *Any*, an *IP address* or an *Object* in case more than one IP address or MAC address needs to be specified. In some sections the *Source* or *Destination* are omitted because their values are already known, for example Zentyal will always be the *Destination* in the *Traffic from internal networks to Zentyal* section and always the *Source* in *Traffic from Zentyal to external networks*

Additionally, each rule is always associated with a *Service* in order to

Additionally, each rule is always associated with a *Service* in order to specify the protocol and the ports (or range of ports). The services with source ports are used for rules related to outgoing traffic of internal services, for example an internal HTTP server. While the services with destination ports are used for rules related to incoming traffic to internal services or from outgoing traffic to external services. Is important to note that there is a set of generic labels that are very useful for the firewall like *Any* to select any protocol or port, or *Any TCP*, *Any UDP* to select any TCP or UDP protocol respectively.

The more relevant parameter is the *Decision* to take on new connection. Zentyal allows this parameter to use three different decisions types.

- Accept the connection.
- Deny the connection, ignoring incoming packets and telling the source that the connection can not be established.
- Register the connection event and continue evaluating the rest of the rules. This way, using *Maintenance ▸ Logs -> Log query -> Firewall* you can check which connections were attempted.

The rules are inserted into a table where they are evaluated from top to bottom. Once a rule accepts a connection, the rest are ignored. A generic rule at the beginning of the chain can have the effect of ignoring a more specific one that is located later in the list, this is why the order of rules is important. You can also apply a *logical not* to the rule evaluation using *Inverse match* in order to define more advanced policies.

Creating a new rule in the firewall

For example, if you want to register the connections to a service, first you use the rule that will register the connection and then the rule that will accept it. If these two rules are in inverse order, nothing will be registered, because the first rule has already accepted the connection. Following the same logic if you want to restrict the access to the Internet, first restrict the desired sites or clients and then allow access to the rest, swapping the location of the rules will give complete access to every client.

By default, the decision is always to deny connections and you have to

add explicit rules to allow them. There are a series of rules which are automatically added during installation to define an initial version of firewall policies: allow all the outgoing connections to external networks to the Internet, from the Zentyal server (in *Traffic from Zentyal to external networks*) and also allow all the connections from internal to external networks (in *Traffic between internal networks and from internal networks to Internet*). Additionally, each installed module adds a series of rules in sections *Traffic from internal networks to Zentyal* and *Traffic from external networks to Zentyal*, normally allowing traffic from internal networks and denying from the external networks. This is made implicit, but it simplifies the firewall management by allowing the service. Only the parameter *Decision* needs to be changed and you do not need to create a new rule. Note that these rules are added during the installation process of a module only, and they are not automatically modified during future changes.

Finally, there is an additional field *Description* used to add a descriptive comment about the rule policy within the global policy of the firewall.

Copyright 2004-2012 Zentyal S.L.

Routing

Zentyal uses the Linux kernel subsystem for the routing, configured using the tool iproute2 [1].

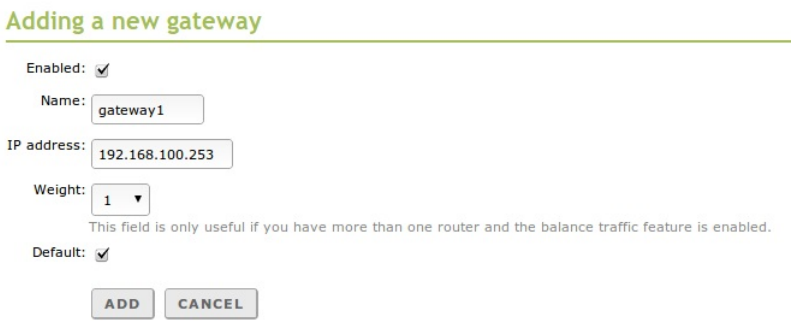
[1] http://www.policyrouting.org/iproute2.doc.html

Configuring routing with Zentyal

Gateway

The *gateway* is the default *router* for the connections associated with a destination that is not in the local network. This means, if the system does not have static routes defined or if none of these match with the desired transmission, the gateway will be used by default.

To configure a gateway in Zentyal go to *Network* ▸ *Gateways*, which contains the following parameters.



Adding a Gateway

Enabled:

Indicates whether this gateway is effectively working or if it is disabled.

Name:

Name used to identify the Gateway.

IP Address:

IP Address of the gateway. This address has to be directly accessible from the host Zentyal is installed on, this means, without other routers in the middle.

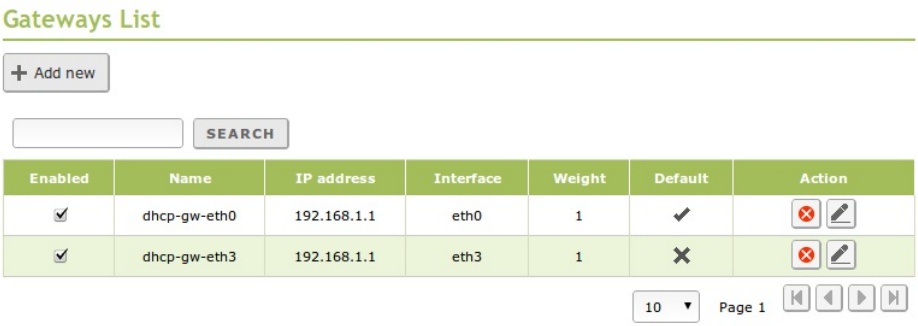
Weight

The heavier the weight, more traffic will be sent using this *gateway* if you have traffic balancing enabled. For example, if the first gateway has a weight of '7' and the second one has a weight of '3', 7 bandwidth units will go through the first one per each 3 bandwidth units that go through the second one, in other words, 70% of the traffic will use the first gateway and the remaining 30% will use the other one.

Default

If this option is enabled, this will be the default gateway.

If you have configured interfaces as DHCP or PPPoE [2] you can not add a gateway explicitly for these, because they are automatically managed. Nevertheless, you can still enable or disable them by editing the *Weight* or choosing whether one of them is the *Default*, but it is not possible to edit any other attributes.



List of gateways

Additionally Zentyal may need a proxy in order to access the Internet, for example, for software and antivirus updates, or for HTTP proxy redirection.

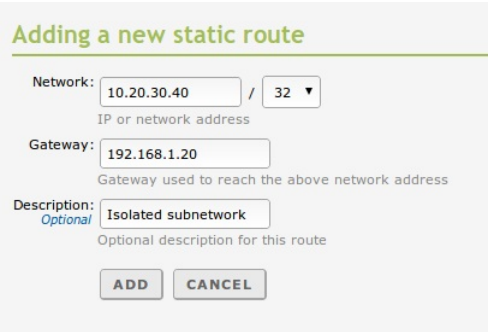
In order to configure this external proxy, go to *Network ▸ Gateways*. Here you can specify the address for the *Proxy server* and also the *Proxy port*. A *User* and *Password* can be specified if the proxy requires them.

[2] http://en.wikipedia.org/wiki/PPPoE

Static route table

If all the traffic directed to a network must go through a specific gateway, a static gateway is added.

For making a manual configuration of a static route, you have to use *Network ▸ Static Routes*.



Static route configuration

These routes can be overwritten if the DHCP protocol is in use.

Copyright 2004-2012 Zentyal S.L.

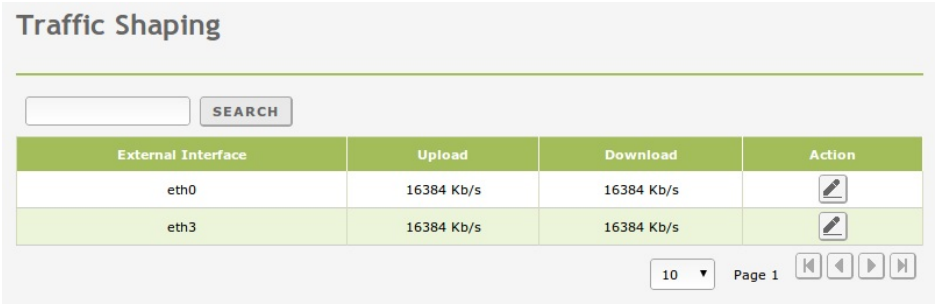
Quality of Service (QoS)

Quality of service configuration in Zentyal

Zentyal is able to perform traffic shaping on the traffic flowing through the server, allowing a guaranteed or limited rate, or assigning a priority to certain types of data connections through the menu *Traffic shaping ‣ Rules*. You need to install and enable the 'Traffic Module' for this.

In order to perform traffic shaping, at least, an internal network interface and an external interface is required.

The first step to configure this module is accessing *Traffic Shaping ‣ Interface Rates* and configuring the upload and download ratios associated with each one of the external interfaces depending on their bandwidth.

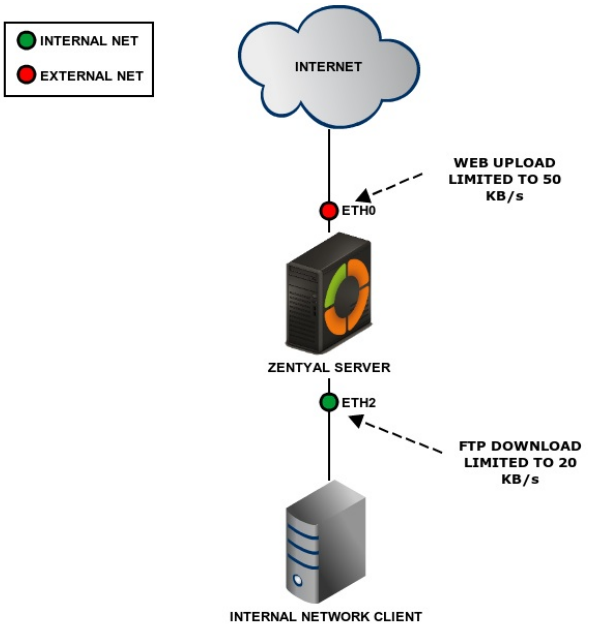


Upload and download rates for the external interfaces

Once you have configured the rates, you can stablish the shaping rules accessing *Traffic Shaping ‣ Rules*, where you can see two different types of rules: Rules for Internal Networks and Rules for External Networks.

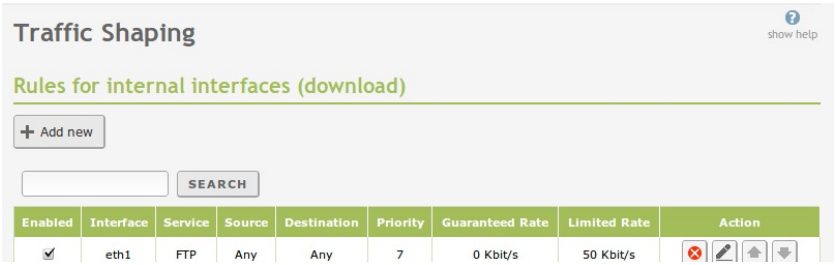
If the external network interface is shaped, from the point of view of the user you are limiting Zentyal output traffic to the Internet. If, however,

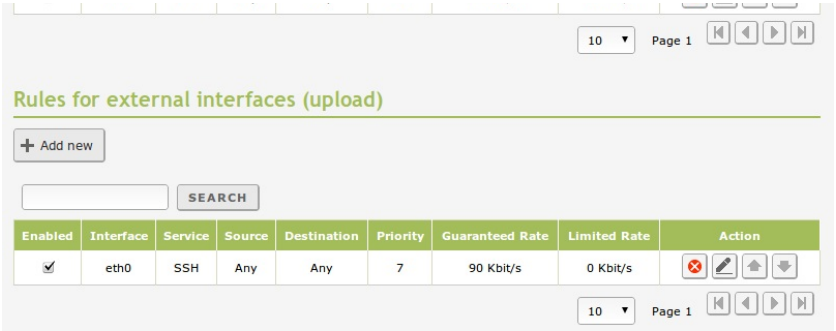
you shape an internal network interface, then the Zentyal output to internal networks is limited. The maximum output and input rates are given by the configuration in *Traffic Shaping* ‣ *Interface Rates*. As you can see, shaping input traffic is not possible directly, because input traffic is not predictable nor controllable most of the time. There are specific techniques taken from various protocols used to handle the incoming traffic. TCP, by artificially adjusting the window size for the data flow in the TCP connection as well as controlling the rate of acknowledgements (ACK) segments being returned to the sender.



Example of traffic shaping rules and their associated interface

You can add rules for each network interface in order to give *Priority* (0: highest priority, 7: lowest priority), *Guaranteed rate* or *Limited rate*. These rules apply to traffic bound to a *Service*, a *Source* and/or a *Destination* of each connection.





Traffic shaping rules

Additionally, it is possible to install the component *Layer-7 Filter* which allows you to configure a more complex analysis of the traffic shaping, based on identifying the last level protocols by their content rather than the port. As you can see when you install this component, you can use this filter by choosing *Application based service* or *Application based service group* as *Service*.

The rules based on this type of filtering are more effective than the ones that just check the port, given that you may have servers configured to provide the service on non-default ports. This will be unnoticed if you do not analyze the traffic itself. It is expected that this type of analysis usually means a heavier processing load for the Zentyal server.

Copyright 2004-2012 Zentyal S.L.

Network authentication service (RADIUS)

Zentyal integrates the FreeRADIUS [2] server, the most popular in Linux environments.

[2] http://freeradius.org/

Configuring a RADIUS server with Zentyal

To configure the RADIUS server in Zentyal, you need first to check in *Module status* if *Users and Groups* is enabled, because RADIUS depends on this. You can create a group from the menu *Users and Groups* ▸ *Groups* and add users to the system from the *Users and Groups* ▸ *Users* menu. While you are editing a group, you can choose the users that belong to it. The configuration options for users and groups are explained in detail in chapter *Directory Service (LDAP)*.

Once you have added groups and users to your system, you need to enable the module in *Module status* by checking the *RADIUS* box.

General configuration of RADIUS

To configure the service, go to *RADIUS* in the left menu. Here you can define if *All users* or only the users that belong to a specific group will be able to access the service.

All the NAS devices that are going to send authentication requests to Zentyal must be specified in *RADIUS clients*. For each one you can define:

Enabled:

Whether the NAS is enabled.

Client:

Name for this client, similar idea to the host name.

IP Address:

The IP address or range of IP addresses from where it is allowed to send requests to the RADIUS server.

Shared password:

Password to authenticate and cypher the communications between the RADIUS server and the NAS. This password must be known for both sides.

Copyright 2004-2012 Zentyal S.L.

HTTP Proxy Service

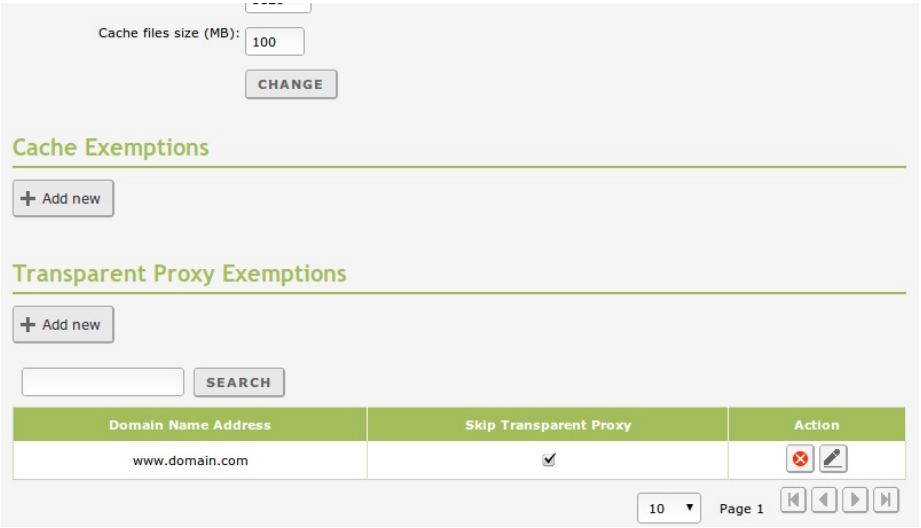
Zentyal uses Squid [1] as HTTP proxy, along with Dansguardian [2] for the content control.

[1] http://www.squid-cache.org/
[2] http://www.dansguardian.org/

HTTP Proxy configuration in Zentyal

To configure the HTTP Proxy, you will go to *HTTP Proxy* ▸ *General Settings*. You can define whether you want the proxy to work in *Transparent mode* to transparently enforce politics, or if it will have to be configured manually in the browsers. In the last case, using *Port*, you can stablish in which port the proxy is going to accept the incoming connections. The default port is TCP/3128, other typical ports are 8000 and 8080. Zentyal's proxy only accepts incoming connections from the internal networks, so that's what you have to configure in the client's browser.

The cache size controls the amount of space in the disk you are going to use to temporarily store web content. It's configured using *Cache Size*. You need a good estimation of the amount and type of traffic you are going to receive to optimize this parameter.



HTTP Proxy

It's possible to configure which domains are not going to be stored in the cache. For example, if you have local web servers, you will not improve the access storing a cache and you will waste memory that could be used for storing remote elements. If a domain is in the cache exemption list, the data will be retrieved delivered directly to the browser. You can define this domains in *Cache exemptions*

Also, you may want to server some web pages directly from the original server, for the privacy of your users or just because they don't operate correctly behind a proxy. For these cases, you can use the *Transparent Proxy Exemptions*.

The feature *Enable Single Sign-On (Kerberos)* will allow you to automatically validate the user, using the *Kerberos* ticket created at session log in. You can find more details of this authentication scheme at *File sharing and authentication service*.

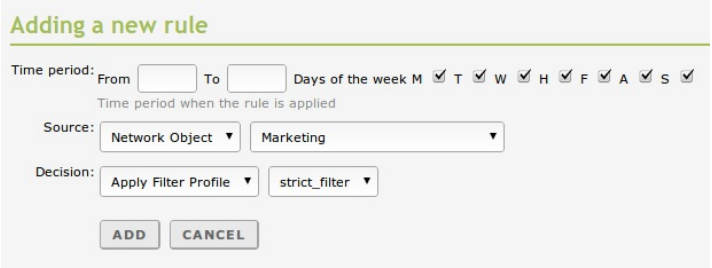
Warning: If you are going to use automatic authentication with *Kerberos*, you have to enter the domain name of the server in the client's browser configuration, never the IP address.

The HTTP Proxy is able to remove the advertisement from the web pages as well. This will save bandwidth and remove distractions, or even security threats. To use this feature you only have to enable *Ad*

Blocking.

Access Rules

Once you have decided your general configuration for the proxy, you have to define the access rules. By default you will find a rule in *HTTP Proxy ▸ Access Rules* which allows all access. Similarly to the *Firewall*, the implicit rule is to deny, and the upper rule will have preference if several can apply to a given traffic.



New access rule in the proxy

Using the *Time Period* you can define in which moment the rule will apply, days of the week and hours. The default is *all times*.

The *Source* is a really flexible parameter, it allows you to configure if this rule will apply to an *Object* or to the members of a specific *Group* (remember that group access rules are only available if you are using a **Non Transparent** Proxy). You can also apply a rule to all the traffic going through the proxy.

Warning: Because of some limitation in DansGuardian it's not possible to perform certain mixes of group-based rules and object-based rules. Zentyal's interface will warn you if it detects one of this cases.

Again, similarly to the *Firewall* once the traffic has matched one of the rules, you have to specify a *Decision*, in the case of the Proxy you have three options:

- Allow all: Accepts all the traffic without making any check, it still allows the user to have a web cache and the administrator to have an access log.
- Deny all: Denies all the connection attempts to the web.

- Apply filter profile: For each request, it will check that the contents don't violate any of the filters defined in the profile, we will talk about the available filters in the next section.

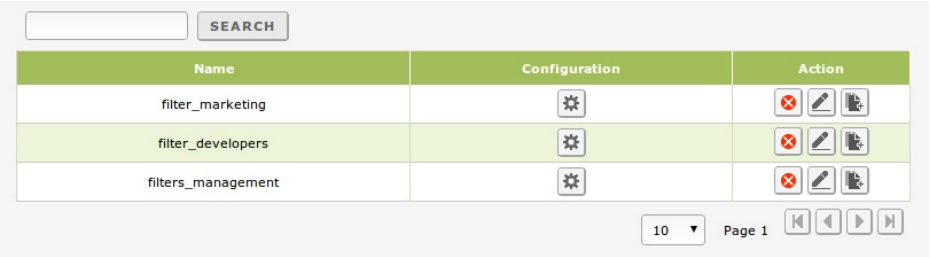
Let's study the following example:

Access rules example

Anyone will be able to access without any restriction during the weekends, because is the upper-most rule. At any other time, the requests coming from the 'Marketing' object will have to be approved by the filter defined in 'strict_filter', the request coming from the object 'Developers' will access without restrictions. The request not matching with any of this rules will be denied.

Filter profiles

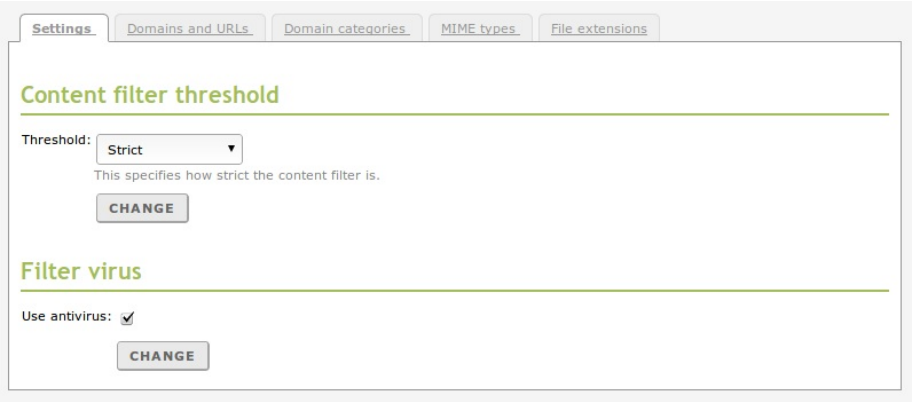
You can filter web pages with Zentyal depending on their contents. You can define several filter profiles from *HTTP Proxy ▸ Filter Profiles*.



Filter profiles for the different objects or user groups

If you go to the *Configuration* of one of this profiles, you can specify different criteria to adjust the content filters. In the first tab you can find the *Threshold* and the antivirus filters. To have the antivirus checkbox

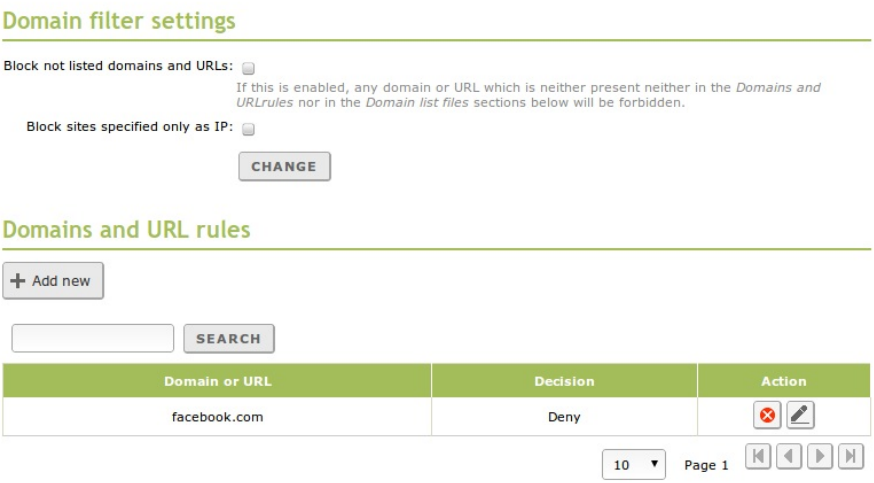
available you need to have the antivirus module installed and enabled.



Filter configuration

This two filters are dynamic, which means that they will analyse any web page to find inappropriate content or viruses. The threshold can be adjusted to be more or less strict, this will influence the number of inappropriate words it will tolerate before rejecting a web page.

In the next tab *Domains and URLs* you can statically decide which domains will be allowed in this profile. You can *Block sites specified only as IP* to avoid bypassing the proxy by just typing IP addresses and you can also decide to *Block not listed domains and URLs* if you want to define a *whitelist* in the domain list below this options.

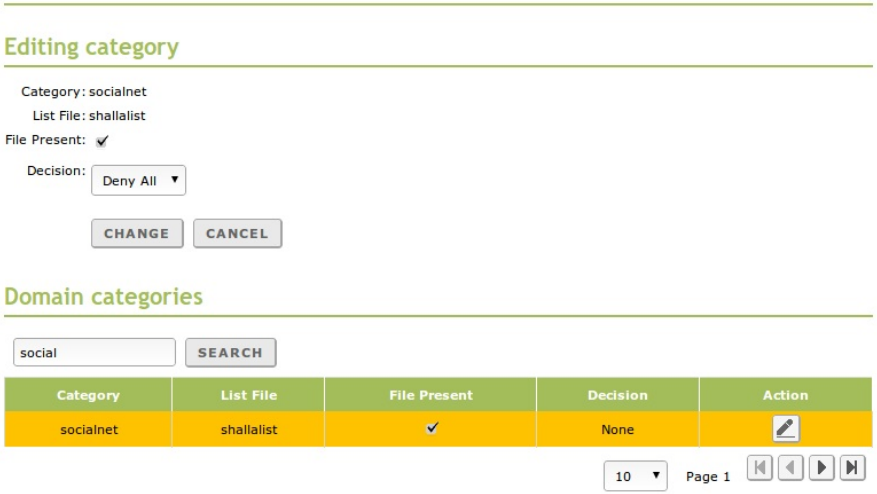

Domain filter settings
Block not listed domains and URLs:
If this is enabled, any domain or URL which is neither present neither in the Domains and URLrules nor in the Domain list files sections below will be forbidden.
Block sites specified only as IP:
CHANGE
Domains and URL rules
Add new
SEARCH
Domain or URL
Decision
Action
facebook.com
Deny
10
Page 1

Finally, at the bottom you have the list of rules, where you can specify which domains you want to accept or deny.

To use the *Domain categories* you need, in first place, to load a categorized domain list. You can load this list from *HTTP Proxy* ▸ *Categorized list*.

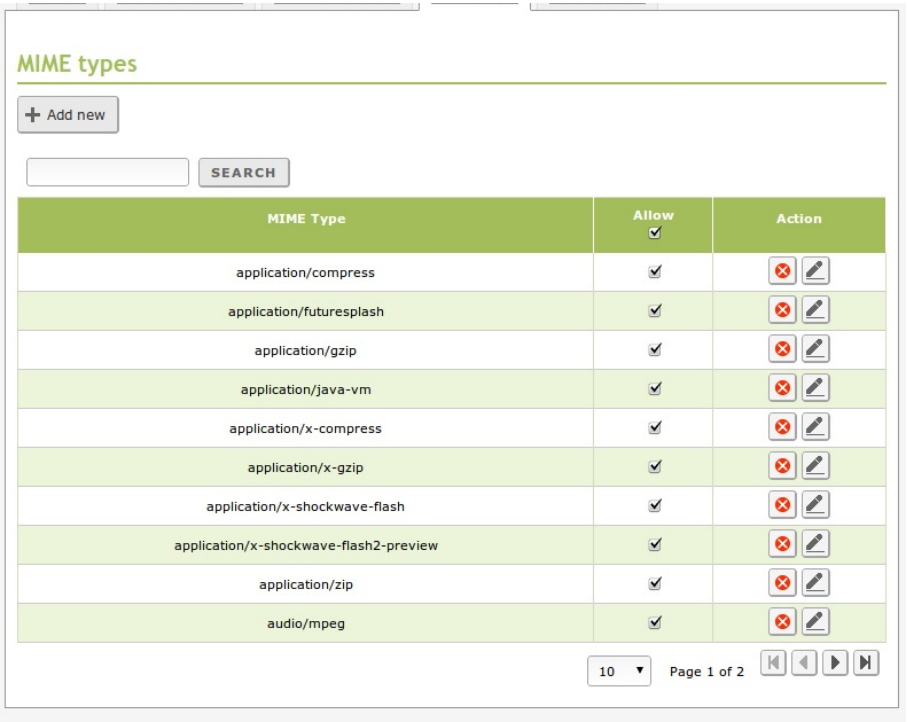
Categorized list

Once you have configured the list, you can choose which category will be denied from *Domain Categories*



Blocking access to social networks

Using the two left tabs you can select which types of contents or files will be accepted by this profile, either using MIME types or file extensions. The MIME [3] types are a format identifier for Internet, for example *application/pdf*.



MIME type filter

As you can see in the image above, the column *Allow* allows you to configure whether the default behaviour will be to deny or to accept a given type.

[3] http://en.wikipedia.org/wiki/Mime_type

You will find a similar interface to configure allowed file extensions:

Blocking '.exe' files

Bandwidth Throttling

Zentyal's Proxy allows you to implement a flexible limit to control the bandwidth used by your users while browsing the web. This limit is based on the *Token Bucket* algorithms [4]. You have a *bucket* with a bandwidth reserve and a refilling speed. The emptying speed will depend on the user's download. If the user uses the connection sensibly, the *bucket* will refill faster than he/she empties it, so there will be no penalization. If the user start to empty the *bucket* much faster than the refilling rate, it will empty and then he/she will have to settle with just the refilling speed.

For each bandwidth throttling rule you configure, you have two types of *buckets* available: global and per client. Each client will consume their personal *buckets* and everyone included in the object will consume the global *bucket*.

Tip: This type of algorithms are useful to allow medium size downloads, if they are not sustained over the time. For example, in an education context, you can allow to download PDFs, this will consume part of the *bucket* but will download at maximum speed. If an user tries to download using P2P, he/she will consume the *bucket* very quick.

Bandwidth Throttling

[4] http://en.wikipedia.org/wiki/Token_bucket

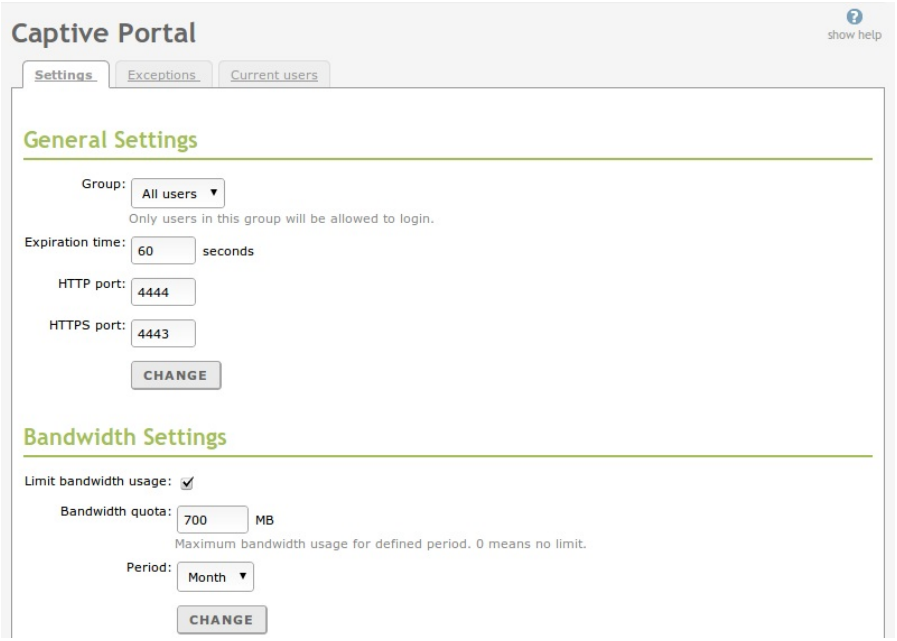
Copyright 2004-2012 Zentyal S.L.

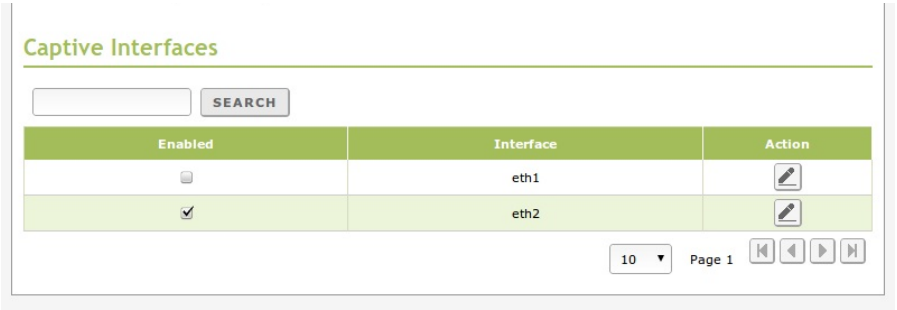
Captive Portal

Zentyal implements a Captive Portal service, which allows you to limit the access to the network from the internal interfaces .

Configuring a captive portal with Zentyal

Through the *Captive Portal* menu you can access the Zentyal's captive portal configuration.





Captive portal configuration

Group

If you define a group, only users belonging to it will be allowed to access through the captive portal. By default access is allowed to all registered users.

HTTP port and *HTTPS port*

You can find the web redirection service under *HTTP port*, and the registration portal in *HTTPS port*. Zentyal will automatically redirect the web requests to the registration portal, located in https://ip_address:https_port/

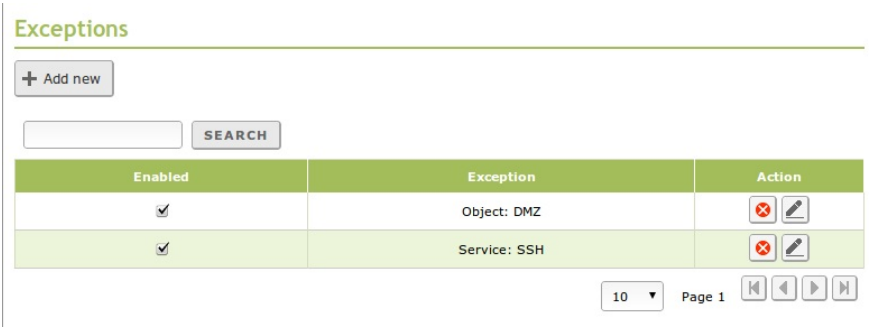
Captive interfaces

Here you can find a list of all the internal network interfaces. The captive portal will limit the access to the interfaces that are checked in this list.

You can also see a form that allows you to limit the bandwidth to a given amount over a given time interval. To use this option, you have to have the module *Bandwidth Monitor* installed and enabled. If you have enabled a limit, after enabling the captive limit over one of the interfaces, the *Bandwidth Monitor* will also be enabled over the same interface. You can see the configuration and reports going to *Network* ▸ *Bandwidth Monitor*.

Exceptions

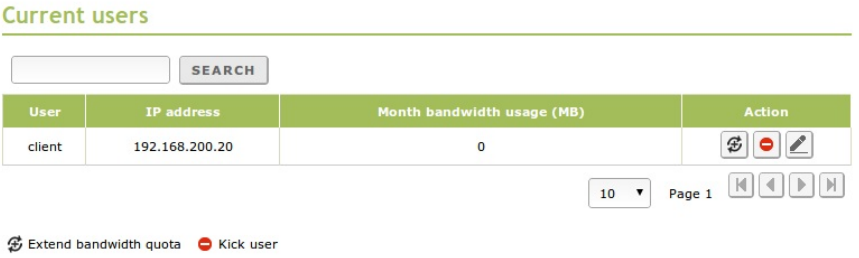
You can set up exceptions to the captive portal, so that certain *Objects* or *Services* will be able to access the external network without having to pass through the log-in forms.



Exceptions to the captive portal

List of Users

The *Current users* tab contains a list of the users which are currently registered in the captive portal.



Current users

The following information for each user is available:

User

Name of the registered user.

IP address

IP address of the user

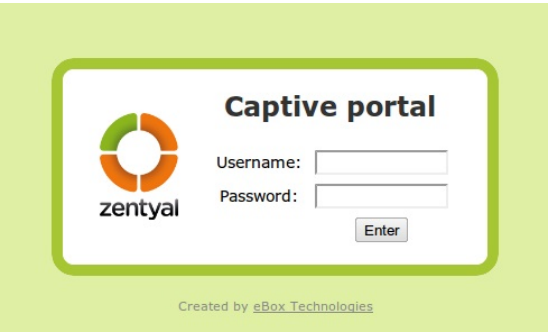
Bandwidth use (Optional)

If the Bandwidth Monitor module is enabled, this field will show the bandwidth use (in MB) of the user for the configured period.

From this list it is also possible to "kick" the users or "Extend Bandwidth Quota" their credit. Kicking the user will instantly close the user's session, leaving him without Internet access. Extending the quota will add the default quota to his/her current credit.

Using the captive portal

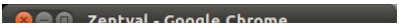
When a user, connected to Zentyal through a captive interface, tries to access any web page using his/her browser, he/she will be automatically redirected to the Captive Portal, asking for authentication.



Captive Portal authentication webpage

After a successful login, a pop-up window will be shown to the user. This window keeps the user session open, so it should be kept open until the user disconnects from the Captive Portal.

Tip: Most browsers will automatically block the *pop-up*, you have to always allow *pop-ups* from Zentyal.



Session window

Copyright 2004-2012 Zentyal S.L.

Intrusion Detection System (IDS)

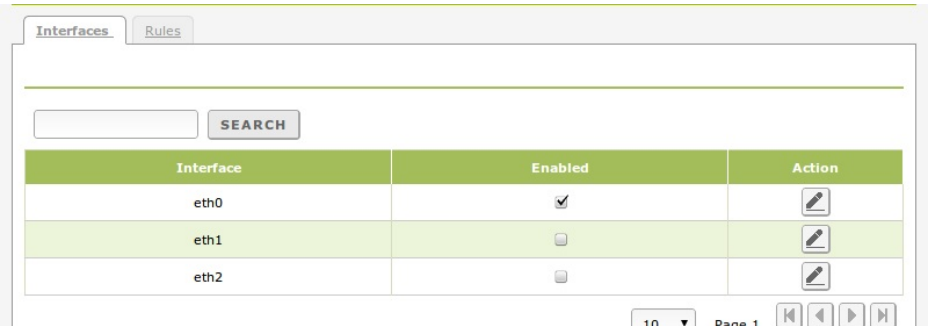
Zentyal integrates Snort [2], one of the most popular IDS, available for both Windows and Linux systems.

[2] http://www.snort.org

Configuring an IDS with Zentyal

Configuration of the Intrusion Detection System in Zentyal is very easy. You only have to enable or disable a number of elements. First, you have to specify which network interfaces you need IDS to listen on. After this, you can choose different groups of rules that will matched to the captured packets in order to obtain alerts, in case of positive results.

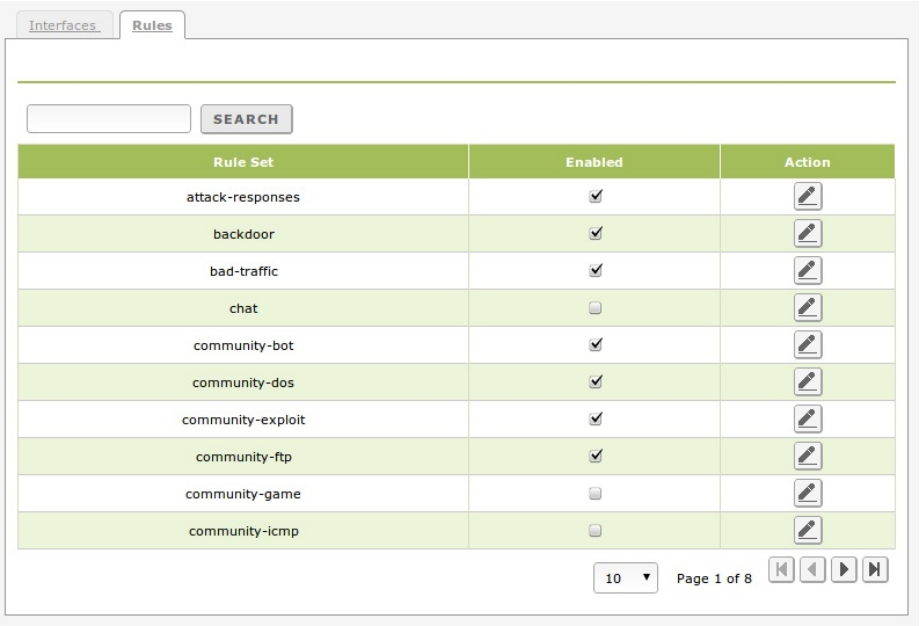
You can access both configuration options through the *IDS* menu. In this section, on the *Interfaces* tab, a table with all the configured network interfaces will appear. All of them are disabled by default due to the increased network latency and CPU consumption caused by the inspection of the traffic. However, you can enable any of them by clicking on the checkbox.



Network interface configuration for IDS

In the *Rules* tab you have a table preloaded with all the Snort rulesets installed on your system. A typical set of rules is enabled by default.

You can save CPU time disabling those rules you are not interested in, for example, those related to services not available in your network. If you have extra hardware resources you can also enable additional rules.



IDS rules

IDS Alerts

So far the basic operation of the IDS module has been described. This is not very useful by itself because you will not be notified when the system detects intrusions and security attacks against the network. As you are going to see, thanks to the Zentyal logs and events system, this notification can be made simpler and more efficient.

The IDS module is integrated with the Zentyal logs module so if the latter is enabled, you can query the different IDS alerts using the usual procedure. Similarly, you can configure an event for any of these alerts

procedure. Similarly, you can configure an event for any of these alerts to notify the systems administrator.

For additional information, see the *Logs* chapter.

Copyright 2004-2012 Zentyal S.L.

Zentyal Office

This section explains some of the services offered by Zentyal as an office server. In particular; its ability to manage network users in a centralised way, the sharing of files and printers, automatized sign-on on different services, web applications and backups for the user data.

Directory services allow you to manage user permissions within an organisation in a centralised way. Meaning that users can authenticate into the network securely. Also, you can define a hierarchical structure controlling the access to the organisation's resources. Finally, thanks to the master/slave architecture integrated within Zentyal, centralised user management can be applied to large organisations with multiple network locations.

File sharing and establishing access control for users and groups, is one of the most important features of an office server and it greatly eases access to workgroup documents in an intuitive way. Security policy allows the protection of critical files within an organisation.

Moreover, many businesses use *Web* applications installed on an HTTP server spanning different domain names allowing HTTPS connections.

Sharing printers, using user and group permissions is also a very important service in any organisation, since this allows you to optimise the resources usage and availability.

Finally, the backups tools for both Zentyal configuration and user's date is without any doubt a critical and indispensable tool in any enterprise server to ensure the recovery process after a failure or mishap

enterprise server to ensure the recovery process after a failure or mishap of your systems, protecting you from data loss and downtime.

Copyright 2004-2012 Zentyal S.L.

Directory Service (LDAP)

Zentyal integrates **OpenLDAP** [3] as a directory service, with **Samba** [4] to implement the domain controller functionality of Windows and also file and printer sharing.

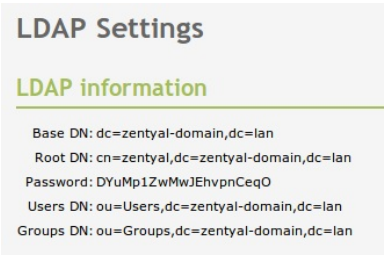
[3] http://www.openldap.org/
[4] http://en.wikipedia.org/wiki/Samba_(software)

Configuration of an LDAP server with Zentyal

LDAP configuration options

Going to *Users and Groups* ▸ *LDAP Settings* you can check the current LDAP configuration and perform some adjustments related to the configuration of PAM authentication on the system.

In the upper part, you can see the *LDAP Information*:



LDAP configuration in Zentyal

Base DN:

Base of the domain names in this server

Base of the domain names in this server.

Root DN:

Domain name of the server root.

Password:

The password of other services and applications that want to use this LDAP server. If you want to configure a Zentyal server as a slave of this server, this is the password that will be used.

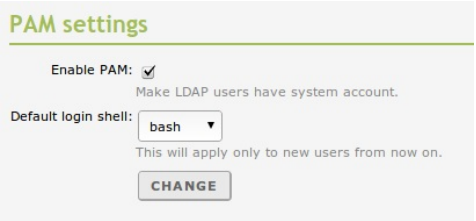
Users DN:

Domain name of the users' directory.

Groups DN:

Domain name of the groups' directory.

In the lower part you can establish some *PAM settings*



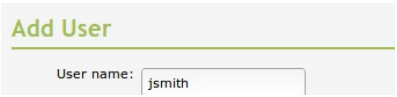
PAM Settings in Zentyal.

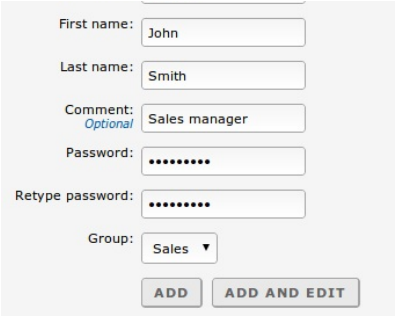
Enabling PAM, you will allow the users managed by Zentyal to also act as normal system users, making possible to start sessions in the server (for example *SSH* and *SFTP*).

In this section you also specify the default command interpreter for your users. This option is initially configured as *nologin*, blocking the users from starting sessions. Changing this options will not modify the existing users in the system, and will only be applied to the users created after the change.

Creating users and groups

You can create users by going to *Users and Groups*▸ *Users* menu and filling the following information:





Adding a user to Zentyal

User name:

Name of the user on the system, it will be the name used in the authentication processes.

Name:

Name of the user.

Surname:

Surname of the user.

Comment:

Additional information about the user.

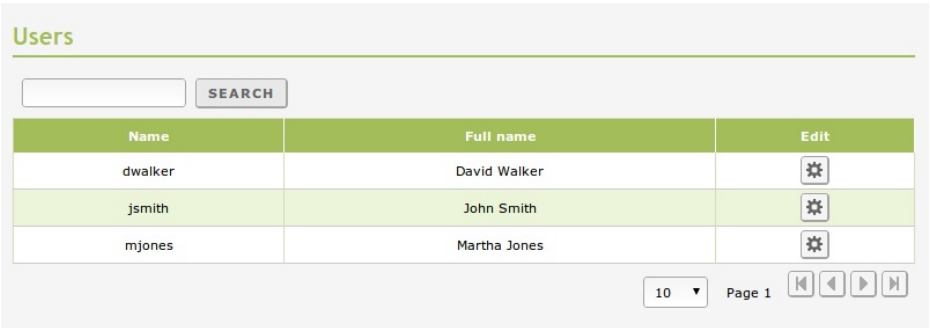
Password:

Password that will be used in the authentication processes. This information will have to be typed twice to avoid typing errors.

Group:

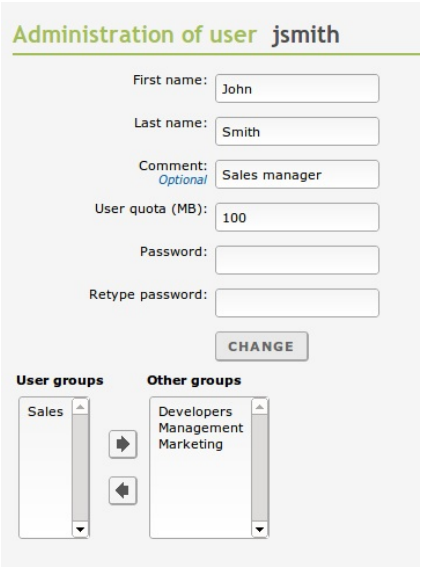
Is possible to add the user to a group during the creation process.

From *Users and Groups* ▸ *Users* you can obtain a list of the users, edit or delete them.



List of users in Zentyal

While editing a user, you can change all the details, except the user name and the information that is associated with the installed Zentyal modules. These contain some specific configuration details assigned to users. You can also modify the list of groups that contain this user.



Editing a user

Editing a user you can:

- Create an account for the jabber server.
- Create an account for the filesharing or PDC with a personalised quota.
- Create an e-mail account for the user and alias for it.
- Assign a telephone extension for the user.
- Enable or disable the user account for Zarafa and check if it has administrator rights.

You can create a group from the *Users and groups* ▸ *Groups* menu. A group will be identified by its name, and can also contain a description.

Adding a group to Zentyal

Going to *Users and groups* ▸ *Groups* you can see all the existing groups, edit or delete them.

While you are editing a group, you can choose the users that belong to the group, and also the information associated with the modules in Zentyal that have some specific configuration associated with user groups.

Editing a group

Among other things, with users groups is possible to:

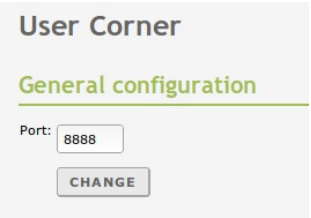
- Have a directory shared between the members of the group.
- Create an alias for a mail address that will forward to all the users of a group.
- Assign access permissions of different *groupware* applications to the users of a group.

User's corner

User editable data

The user's data can only be modified by the Zentyal administrator, which can be inefficient when the number of users to be managed

becomes too big. Administration tasks like changing the password of a user can be very time consuming. For this reason, you need the **User's corner**. This corner is a Zentyal service designed to allow the users to change their own data. This functionality has to be enabled like the rest of the modules. The user's corner is listening on another port different to other processes to enhance the system security.



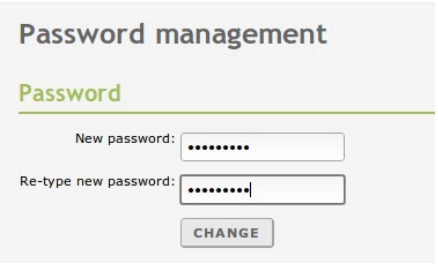
Configure user's corner port

The user can access the User corner using the URL:

https://<Zentyal_ip>:<usercorner_port>/

Once the user enters his/her name and password, he/she can perform changes in his personal configuration. User's corner offers the following functionality:

- Change the current password.
- Configure the voice mail for the user.
- Configure an external personal account to retrieve the mail and synchronise it with the content of the mail server in Zentyal.



Change the current password in user's corner

Copyright 2004-2012 Zentyal S.L.

File sharing and authentication service

Zentyal uses Samba [4] to implement SMB/CIFS and manage the domain, Kerberos [5] for the authentication services.

[4] http://en.wikipedia.org/wiki/Samba_(software)
[5] http://en.wikipedia.org/wiki/Kerberos

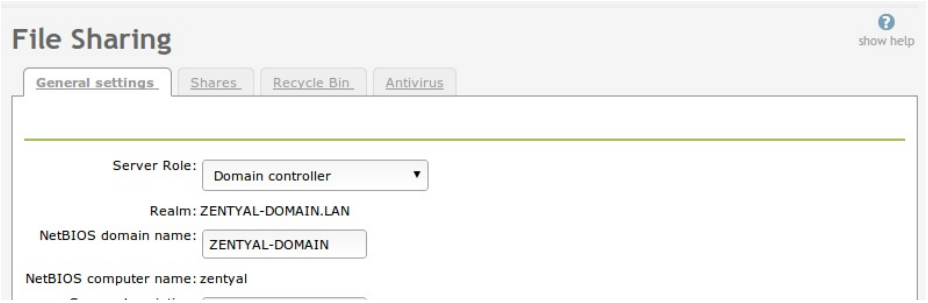
Configuring a file server with Zentyal

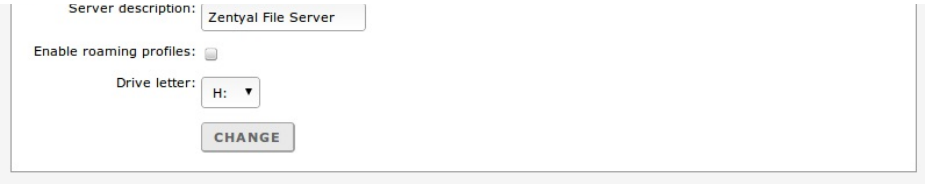
The file-sharing services are active when the **file sharing** module is active, even if the *Domain Controller* function is not.

File sharing is integrated with users and groups. Each user has a personal directory and each group can be assigned a shared directory.

The user's personal directory is automatically shared and can only be accessed by the user.

To configure the general settings of the file sharing service, go to *File Sharing* ▸ *General configuration*.

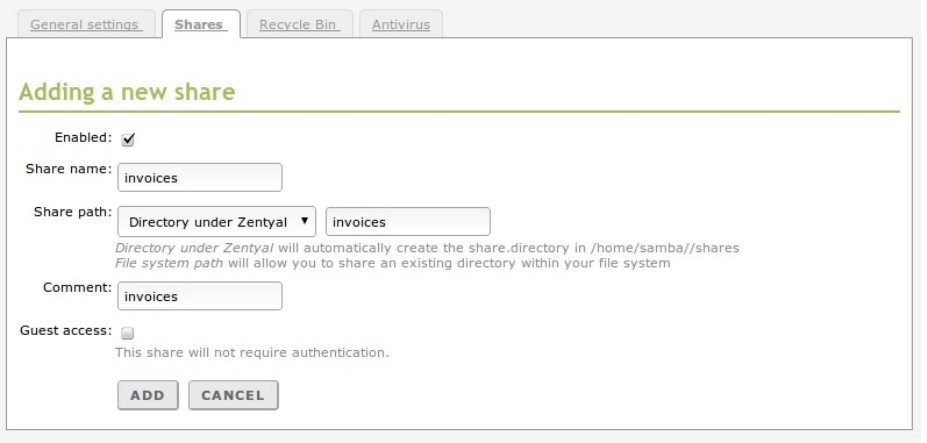




General configuration of file sharing

The *domain* is set to work within the *Windows* local network, and the *NetBIOS name* is used to identify the Zentyal server. You can use a long *description* to describe the domain.

To create a shared directory, use *File Sharing* ▸ *Shares* and click *Add new*.



Adding a new share

Enabled:

Leave it checked if this directory needs to be shared. Disable to stop sharing.

Share name:

The name of the shared directory.

Share path:

Directory path to be shared. You can create a sub-directory within the Zentyal specific directory */home/samba/shares*, or use an existing file system pathway by selecting *Filesystem path*.

Comment:

A more detailed description of the shared directory simplifies management of shared assets.

Guest access:

Enabling this option allows a shared directory to be accessible without authentication. Any other access settings will be ignored.

List of shares

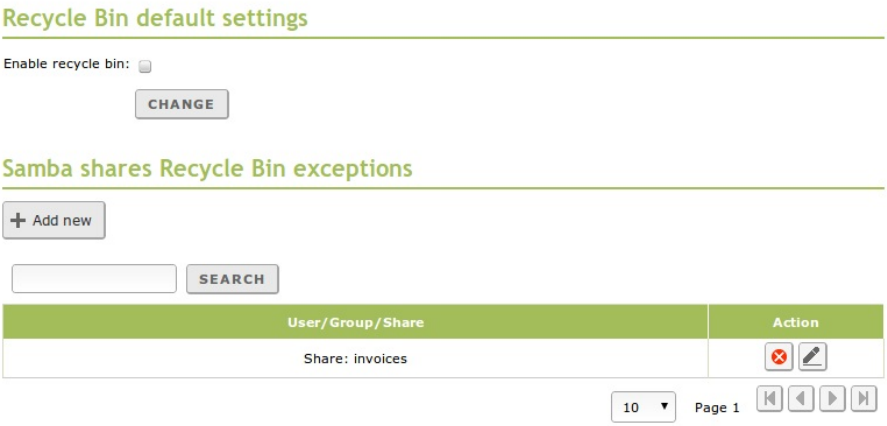
Shared directories can be edited using *Access control*. By clicking on *Add new*, you can assign read, read/write or administration permissions to a user or group. If a user is a shared directory administrator, he/she can read, write and delete any user files within that directory.

Adding a new ACL (Access Control List)

You can also create a share for a group using *Users and Groups* ▸ *Groups*. All group members will have access: they can write their own files and read all the files in the directory.

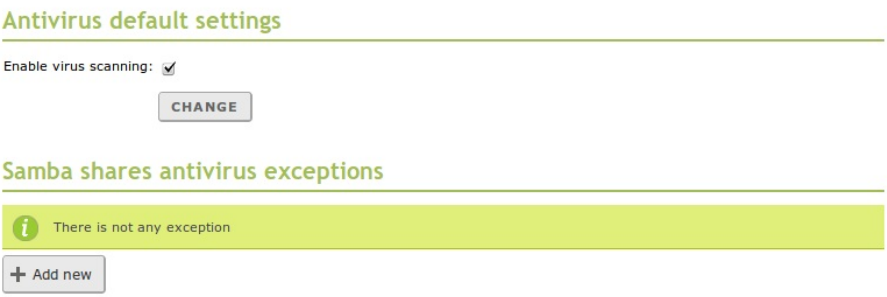
Creating a shared directory for the group

If you want to store deleted files in a special directory called *RecycleBin*, you can check the *Enable recycle bin* box using *File Sharing* ▸ *Recycle bin*. If you do not want to use this for all shared resources, add exceptions using *Resources excluded from Recycle Bin*. Other default settings for this feature, such as the directory name, can be modified using the file `/etc/zentyal/samba.conf`.



Recycle bin

Using *File Sharing* ▸ *Antivirus* virus scanning of shared resources can be enabled and disabled. Exceptions can also be defined where virus scanning is not required. To use this feature the Zentyal **antivirus** module must be installed and enabled.

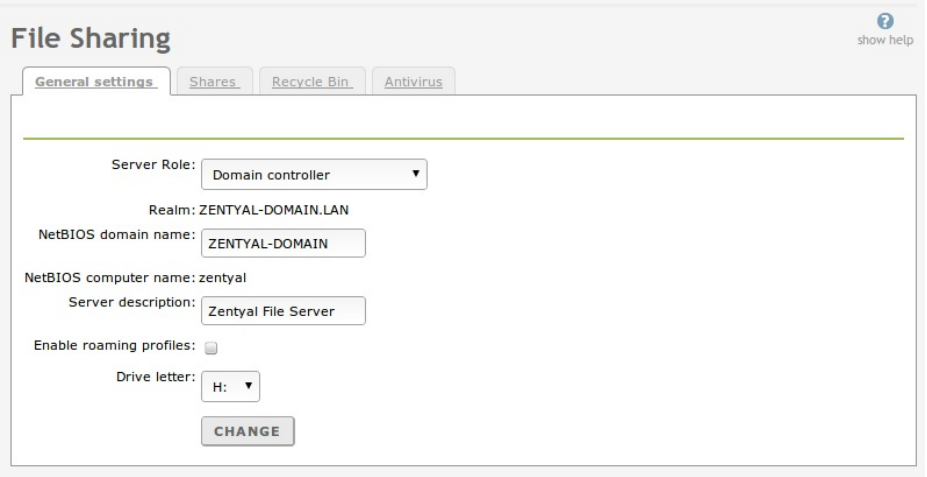


Antivirus scanning shared folders

Configuring a Domain Controller with

Configuring a Domain Controller with Zentyal

Zentyal can act as a Domain Controller, either as the original Controller for this domain or as an *Additional Controller* of an existing *Active Directory* domain.



Authentication server

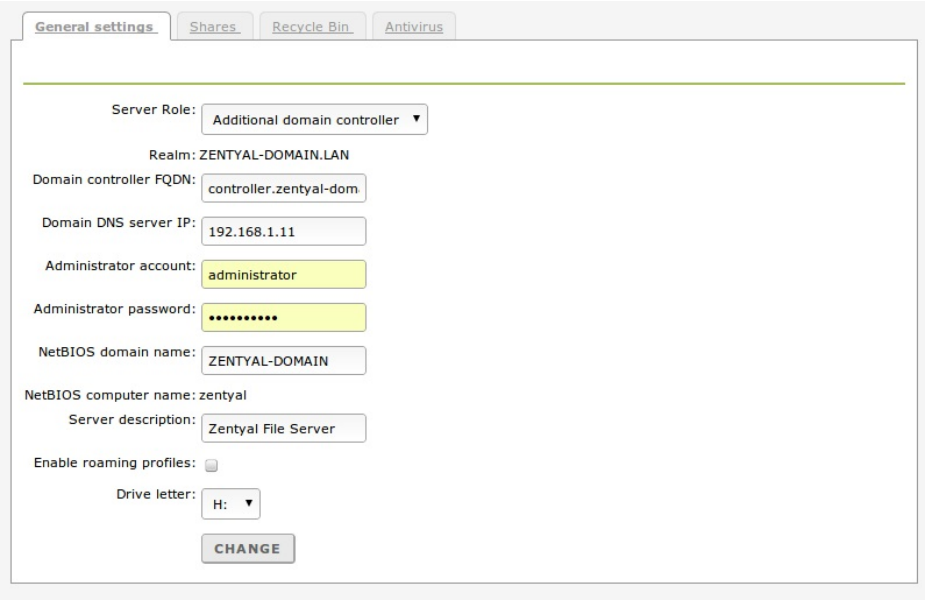
If the *Roaming Profiles* option is enabled, the server will not only authenticate users, but will also store their profiles. These profiles contain all the user information, including Windows preferences, Outlook email accounts and the *Documents* folder.

When a user logs in, the user profile will be retrieved from the domain controller. Therefore, the user will have access to their work environment on multiple computers. Before enabling this option, you must consider that the user information can be several gigabytes in size.

You can also configure the *drive letter* to which the personal user directory will be linked after authenticating against the domain.

If you want to configure your Zentyal server as an *Additional Domain Controller* of an existing *Active Directory* , you will have to go to *General Settings* tab of the *File Sharing* menu. Here you will choose the *Additional Domain Controller* option, the FQDN name of the controller you want to join, the IP address of the DNS server that manages the domain, and finally, username and password needed to

manages the domain, and finally, username and password needed to join.



Zentyal as an Additional Domain Controller

Copyright 2004-2012 Zentyal S.L.

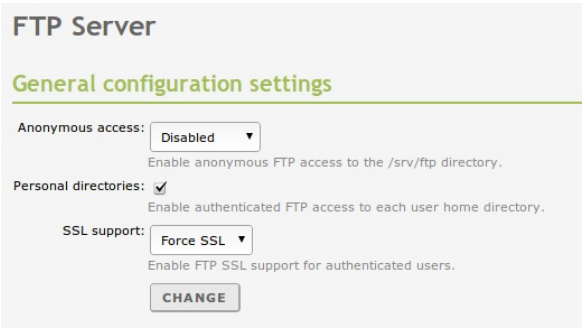
File Transfer Protocol (FTP)

Zentyal uses **vsftpd** [5] (*very secure FTP*) to provide this service.

[5] http://vsftpd.beasts.org/

FTP server configuration with Zentyal

You can access the FTP server configuration through the menu *FTP*:



FTP Server Configuration

The FTP service provided by Zentyal is very easy to configure and it allows the provision of remote access to a public directory and/or personal directories of the system users.

The default path of the public directory is */srv/ftp* while all users have personal directories located within */home/user/*.

I n *Anonymous access* you can choose between three possible

configurations for the public directory:

Disabled:

No access is granted to anonymous users.

Read only:

Users can access the directory with an FTP client, but users are only allowed to list the files and download them. This configuration is appropriate when making content globally available for download.

Read and write:

Users can access the directory with a FTP client and anyone can add, modify, download and delete files from this directory. This configuration is not recommended unless you are very confident of what you are doing.

Another configuration parameter *Personal directories* allows each Zentyal user access to their personal directory. In this case, you can also activate *Restrict to Personal directories*, which will prevent users to navigate the entire file system, only accessing the files and directories under */home/user*.

Using the *SSL Support* option, you can force the secure connection, make it optional or disable it. If it is disabled you will not be able to access securely, if it is optional the decision will depend on the client support and if it is forced, you will not accept clients that do not support it.

As usual, before enabling this service, you must check that the neccesary firewall ports are open.

Warning: You will need to enable *PAM* to allow your LDAP users to access the FTP server.

Copyright 2004-2012 Zentyal S.L.

Web publication service (HTTP)

Introduction to HTTP

The **Web** [1] is one of the most common services on the Internet, to the extent that it has become the "public face" of the *Internet* for most users. This service is based on web page transfer using the HTTP protocol.

HTTP (Hypertext Transfer Protocol) [2] is a request and response protocol. The client, also known as the *User Agent*, makes a request to access a resource on a HTTP server. The server with the requested resource processes it and gives a response with the resource, this can be an HTML web page, image or any other file that is generated dynamically - based on a series of request parameters. These resources are identified by using URLs (*Uniform Resource Locators*) [3] , identifiers usually know as web site addresses.

A client request follows this format:

- Initial line with *<method> <URL> <HTTP version>*. For example, the *GET /index.html HTTP/1.1* requests the resource */index.html* using GET and by using the HTTP/1.1 protocol.
- A line, with headers, such as *Host*, *Cookie*, *Referer* or *User-Agent* amongst others. For example *Host: zentyal.com* informs that a request is made to the domain zentyal.com.
- A blank line.
- A body with optional format, used, for example, to send data to

the server using the POST method.

The *Host* header is used to specify which domain you need to send the HTTP request. This allows different domains with different web pages to exist on the same server. The domains, therefore, will be resolved to the same IP address of the server - after reading the *Host* header the server can designate the virtual host or domain to which the request is addressed.

There are several methods that clients can use to request data, although the most common ones are GET and POST:

GET:
: Requests a resource. It is a harmless method as far as the server is concerned and does not cause any changes to the hosted web applications.

HEAD:
: Requests data from a resource, like GET, but the response will not include the the body, only the header. Hence, it allows you to obtain metadata from the resource without downloading it.

POST:
: Sends data to a resource that the server must process, through a web form, for instance. The data is included in the body of the request.

PUT:
: Sends an item to be stored on a specific resource. It is used, for example, by WebDAV [4], a set of HTTP protocol methods which allow collaboration between users when editing and managing files.

DELETE:
: Deletes the specified resource. Also used by WebDAV.

TRACE:
: Informs the server that it must return the header sent by the client. This is useful to see whether the request has been modified on its way to the server, for example by an HTTP Proxy.

The server response has the same structure as the client request, except for the first line. The first line contains *<status code> <text reason>*

for the first line. The first line contains *<status code> <text reason>*, which is the response code and textual explanation of it.

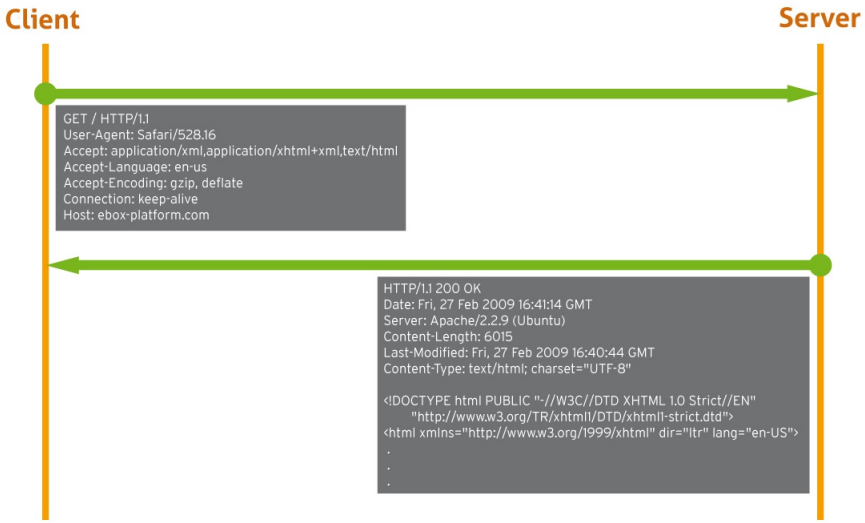
The most common response codes are:

200 OK:
: The request has been processed correctly.

403 Forbidden:
: The client does not have permission to access the requested resource.

404 Not Found:
: The requested resource was not found.

500 Internal Server Error:
: Server error has occurred, preventing the correct processing of the request.



Request schema and HTTP response

By default, HTTP uses the TCP port 80 and HTTPS uses the TCP port 443. HTTPS is the HTTP protocol sent via SSL/TLS connection to guarantee encrypted communication and authentication of the server.

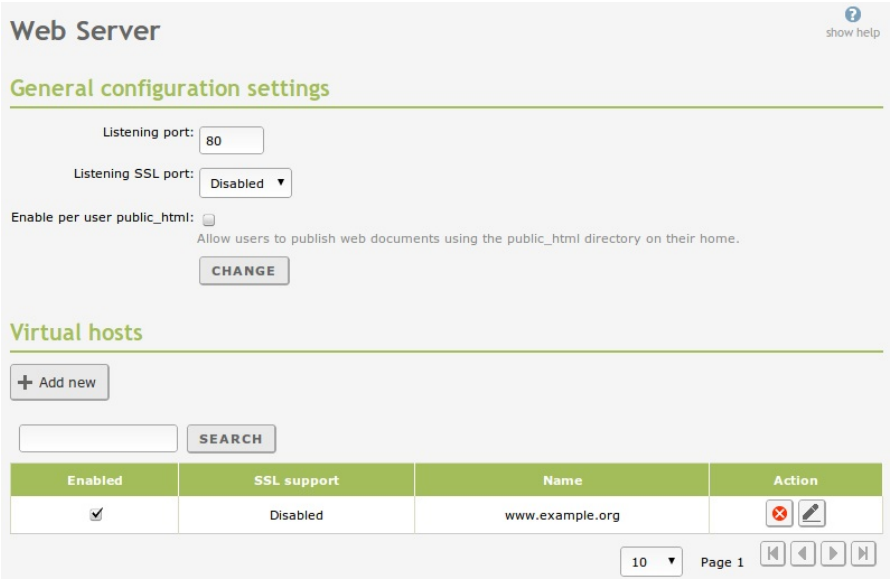
The **Apache** [5] HTTP server is the most widely used on the Internet

The **Apache** [3] HTTP server is the most widely used on the Internet, hosting more than 54% of all web pages. Zentyal uses Apache for its HTTP server module and for its administrative interface.

[1] http://en.wikipedia.org/wiki/World_Wide_Web
[2] http://en.wikipedia.org/wiki/HTTP
[3] http://en.wikipedia.org/wiki/URL
[4] http://en.wikipedia.org/wiki/WebDAV
[5] http://httpd.apache.org/

HTTP server configuration with Zentyal

You can access to the HTTP server configuration through the *Web server* menu.



Configuration of Web server module

In the *General Configuration* you can modify the following parameters:

Listening port:

HTTP port, by default port 80, the default port of the HTTP

protocol.

SSL listening port:

HTTPS port, by default port 443, the default port of the HTTPS protocol. You must enable the certificate for this service and change the Zentyal administrative interface port to another port if you want to use the port 443.

Enable the *public_html* per user:

If the users have a subdirectory called *public_html* in their personal directory, this option allows them to access it via the URL *http://<zentyal>/~<user>/*.

Virtual servers or *Virtual hosts* is where you can define different domains associated to certain web pages. When you use this option to define a new domain, if the DNS module is installed, then the top level domain will be created. If a subdomain does not already exist, then it will be added. This domain or subdomain creates a pointer to the address of the first internal interface configured with a static address - although you can modify the domain later if necessary.

Besides being able to enable and disable each domain of the HTTP server, if SSL has already been configured, you can fix HTTPS connections to a domain or even force all the connections to work over HTTPS.

The *DocumentRoot* or root directory for each page is in the `/srv/www/<domain>/` directory. In addition, it is possible to apply a customised Apache configuration to each *Virtual host* by adding a file to the `/etc/apache2/sites-available/user-ebox-<domain>/` directory.

Copyright 2004-2012 Zentyal S.L.

Printers sharing service

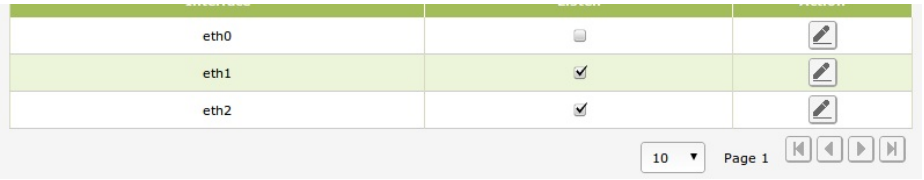
For the management of printers and their access permissions, Zentyal integrates *Samba*, as described in the *Configuring a file server with Zentyal* section. As a printing system, in coordination with *Samba*, Zentyal integrates **CUPS** [1] (Common Unix Printing System).

[1] http://en.wikipedia.org/wiki/Common_Unix_Printing_System

Printer server configuration with Zentyal

In order to share a printer in your network and allowing or denying users and groups access, you need to have access to a printer from a host running Zentyal. This can be done through direct connection, parallel port, USB or through the local network. Besides that, you will need to know the following information; the manufacturer, the model and the driver a printer uses in order to obtain good results during operation.

First, it is worth noting that the configuration and maintenance of printers is not through the Zentyal interface but from the CUPS interface. If you manage the Zentyal server locally then you do not need to do anything special, but if you want to give access to other machines on the network you must explicitly allow access to the network interface, by default, CUPS will not listen to it for security reasons.



Printer management

The CUPS management port is by default 631 and you can access the management interface by using the HTTPS protocol via the network interface on which you have enabled CUPS to listen to. *localhost* can be used if you are operating directly on the Zentyal host.

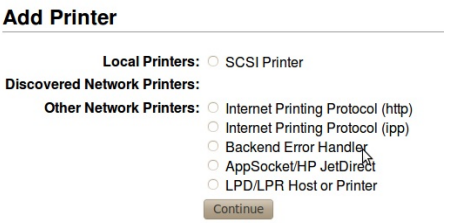
https://zentyal_address:631/admin

For convenience, if you are using the Zentyal interface, you can access CUPS directly through the *CUPS web interface* link.

For the authentication use the same username and password with which you use to access the Zentyal interface.

Once you have logged onto the CUPS administration interface, you can add a new printer through *Printers* ▸ *Add printer*.

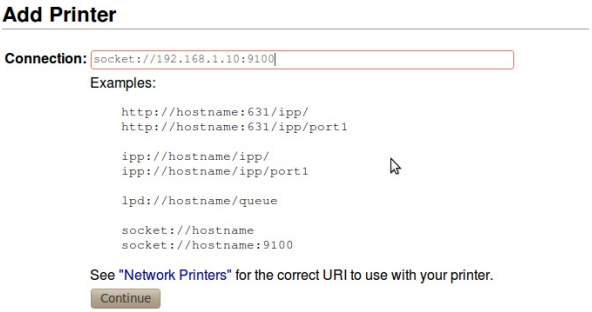
The first step of the wizard used to add a new printer is, select the type of printer. This method depends on the printer model and how it is connected to your network. CUPS also provides a feature for the automatic discovery of printers. Therefore, in most cases it is possible that your printer is automatically detected thus making the configuration easier.



Add printer

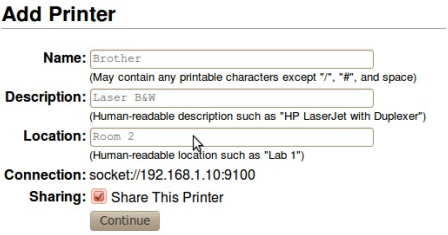
Depending on the method you have selected, you might need to configure the connection parameters. For example, for a network

printer, you must establish the IP address and the port as shown in the image.



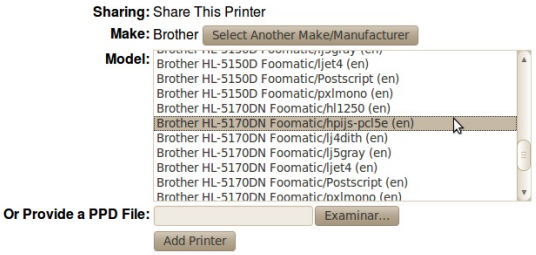
Connection parameters

In the next step, you can specify the printer's name that will be used to identify it later on, together with other additional descriptions of its features and placement. These descriptions can be any character string and their value will be only informational. On the other hand, the name can not include spaces nor special characters.


Add Printer
Name: Brother
(May contain any printable characters except "/", "#", and space)
Description: Laser B&W
(Human-readable description such as "HP LaserJet with Duplexer")
Location: Room 2
(Human-readable location such as "Lab 1")
Connection: socket://192.168.1.10:9100
Sharing: Share This Printer
Continue

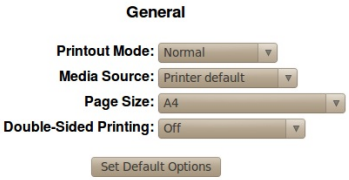
Name and description

Later, you must set the manufacturer, model and which printer driver to use. Once you have selected the manufacturer, a list of available models will appear, with different drivers for each model on the right, separated by a slash. You also have the option to upload a PPD file provided by the manufacturer, if your printer model does not appear on the list.



Manufacturer and model

Finally, you will have the option to modify the general settings.



General settings

Once you have completed the wizard, your printer will be configured. You can check which printing jobs are pending or on progress through *Jobs ▸ Manage jobs* within the CUPS interface. You can perform many other actions, such as print a test page. For more information about printer management with CUPS it is recommended to read the official documentation [3].

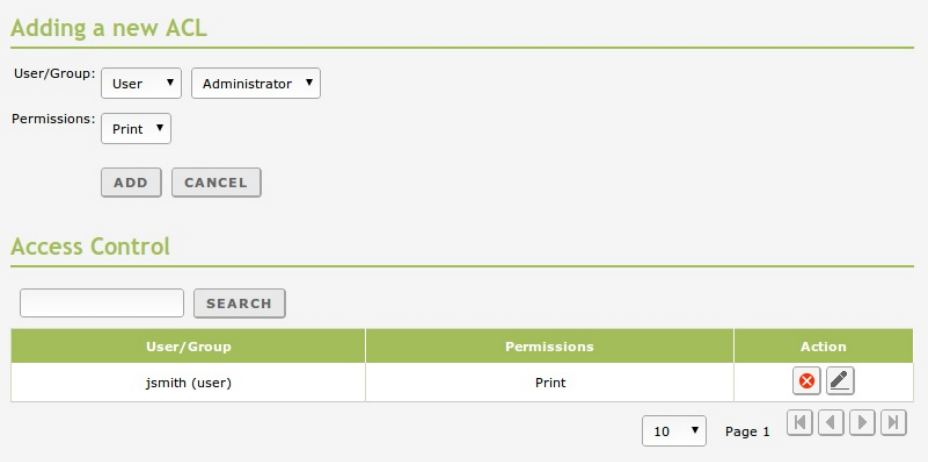
[3] http://www.cups.org/documentation.php

Once the printer has been added through CUPS, Zentyal can export it by using Samba.

You can see the list of available printers at the bottom of *Printer Sharing*

Available printers

Clicking on the *Access Control* button of the printer you can configure the access control list, *ACL*, for this printer.



Available printers

Copyright 2004-2012 Zentyal S.L.

Backup

Zentyal configuration *Backup*

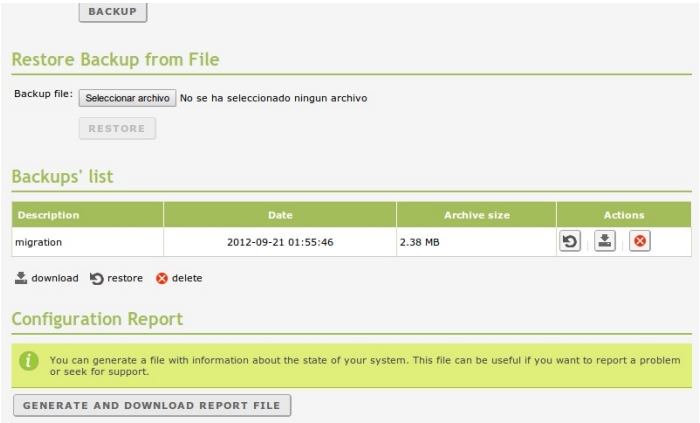
Zentyal offers a configuration *backup* service, to ensure the recovery of a server when a disaster occurs, for example a hard disk failure or a human error while managing configurations.

Backups can be made locally, saving them on the local hard drive of the Zentyal host. After this, it is recommended to save them to an external physical system, so if the machine suffers a failure, you still have access to this data.

It is also possible to automatically perform the *backups* using a commertial version of Zentyal. Both the **Small Business** and the **Enterprise** version include seven configuration backups in the cloud and the cloud **Disaster Recovery** service. Even if you register the Zentyal server for free, you will have one cloud configuration backup. Using any of this options you will be able to quickly recover your Zentyal configuration from the remote servers in the event of a total system failure.

To access the backup options, go to *System* ‣ *Import/Export configuration*. You can not backup if there are unsaved changes in the configuration.

Import/Export Configuration
show help
Local
Remote
Those modules which have not been enabled for first time in the Module Status section will be ignored in both backup and restore operations.
Backup the Current State
Description:
second_migration



Configuring the backup

Once you have entered the *Name* for the backup, chosen the type of backup (incremental or full) and clicked on *Backup*, you will see a window which will show the progress of the different modules until the message **Backup successfully completed** is displayed

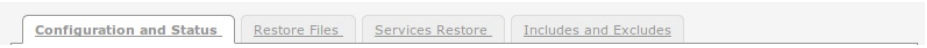
Afterwards, if you return to the former window, you can see in the bottom of the page a *Backups list*. Using this list you can restore, download to a client disk or delete any of the saved copies. Additionally, you will have data about the creation date and size.

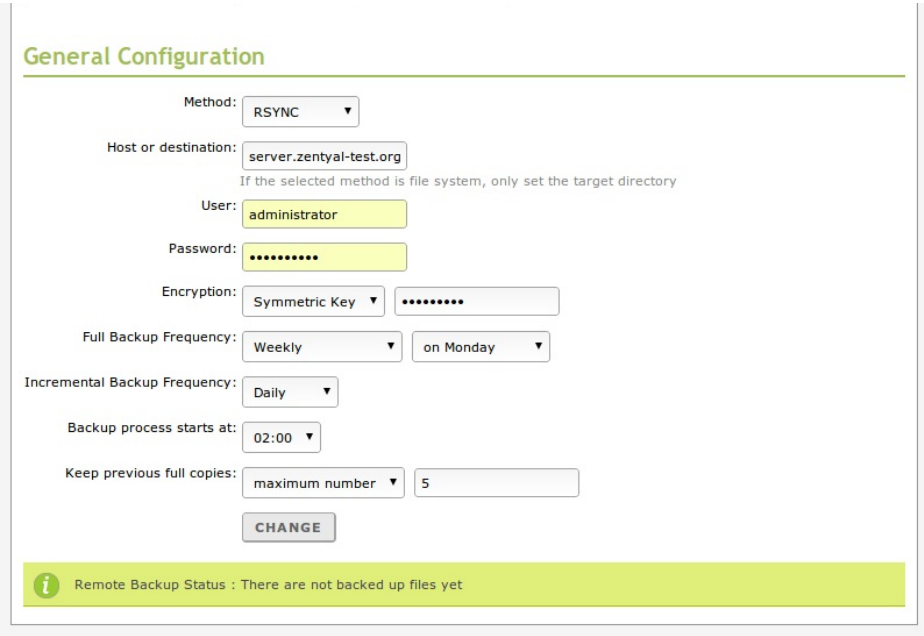
In the *Restore backup from a file* section you can send a security copy file that you have previously created, for example, associated with a former Zentyal server installation in another host and restore it using *Restore*. You will be asked for confirmation; simply remember to be careful, as the current configuration will be completely overwritten. The restoration process is similar to the copy; after showing the progress, the user will be notified with a success message if there is no error.

Data backup configuration in a Zentyal server

You can access the data backup menu going to *System* ▸ *Backup*

First of all, you have to decide whether you are going to store your backups locally or remotely. In the latter case, you need to specify which protocol is going to be used to connect the remote server.





Data backup configuration

Method:

The different supported methods are *FTP*, *Rsync*, *SCP* and *File system*. Take into account that depending on the method you choose, you will have to provide more or less information. All the methods except *File system* use remote servers. If you select *FTP*, *Rsync* or *SCP*, you will have to enter the associated authorisation to connect with the server and the remote server's address.

Warning: When using *SCP*, you have to run *sudo ssh user@server* and accept the server fingerprint in order to add to the list of servers known by SSH. If you do not perform this operation, the backup will not work, because the connection with the server will fail.

Host or destination:

For *remote methods* you have to enter the remote server name or its IP address with the following format: `other.host:port/existing_directory` In case you are using *File system*, you only need the local directory path.

User:

User name to authenticate in the remote host.

Password:

Password to authenticate in the remote host.

Encryption:

You can cypher the data in the backup using a symmetric key that will be entered in the form.

Full Backup Frequency

This parameter is used to determine the frequency for complete backups to be performed. The values are: *Only the first time*, *Daily*, *Weekly*, *Twice a month* and *Monthly*. If *Weekly*, *Twice a month* or *Monthly* is selected, you will see a selection option to choose the exact day of the week or month to perform the backup.

I f *Only the first time* is selected, then it is mandatory to set a frequency for incremental backups.

Incremental Backup Frequency

This value sets the frequency of the incremental copy or disables it.

If the incremental copy is enabled, you can choose a *Daily* or *Weekly* frequency. In the latter case, you have to decide the day of the week; either way you have to take into account the chosen frequency which has to be greater than the full backup.

The days that you have scheduled a full backup, Zentyal will not perform any scheduled incremental copy.

Backup process starts at

This field is used to set the time a backup copy is started, for both the full and the incremental backup. It is a good idea to set it to a time frame where no other activities are being performed in the network, because it can consume a lot of upstream bandwidth.

Keep previous full copies

This value is used to limit the total number of copies that can be stored. You can limit by number or by age.

If you limit by number, only the set number of copies, plus the last complete copy will be stored. If you limit by age, you will only save full copies that are newer than the indicated period.

When a full copy is deleted, all the incremental copies associated with it are also deleted.

Configuration of the directories and files that are saved

From the *Includes and Excludes* tab you can configure the specific data you want to backup.

The default configuration will perform a copy of all the file system except the files and directories explicitly excluded. In case you are using the method *File system*, the destination directory and all its contents will be excluded as well.

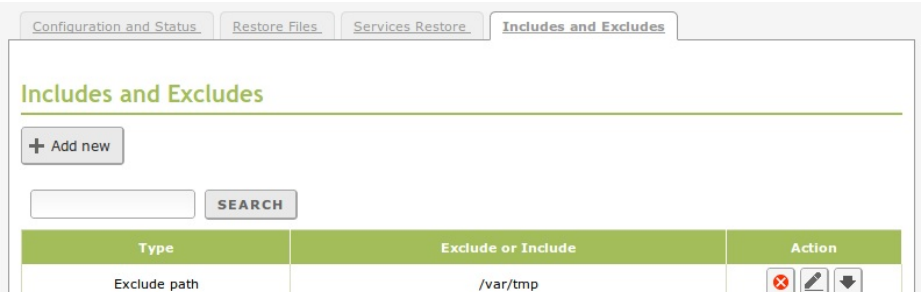
You can set path exclusions and exclusions that match a regular expression. Exclusions by regular expression will exclude any path which matches the expression. Any excluded directory will also exclude all its contents.

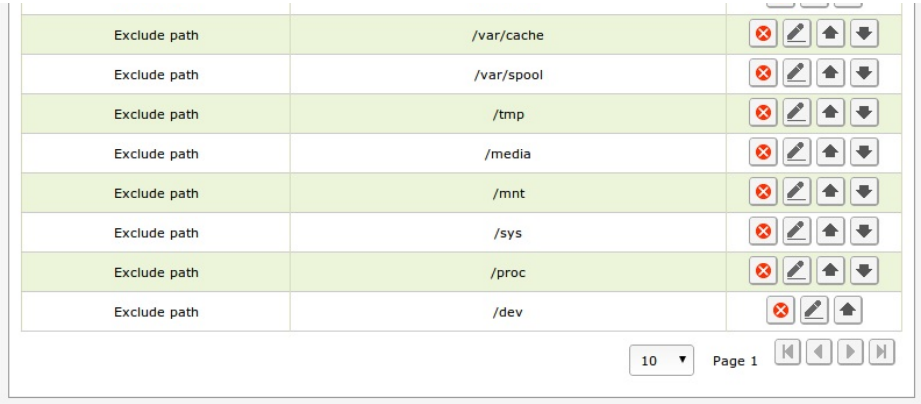
In order to further refine the backup contents, you can also define *inclusions*, when the path matches an inclusion before it matches with an exclusion, it will be included in the backup.

The order of application of inclusions and exclusions can be changed using the arrow icons.

The default list of excluded directories is: `/mnt`, `/dev`, `/media`, `/sys`, `/tmp`, `/var/cache` and `/proc`. It is a bad idea to include any of these directories, because they may cause the backup process to fail.

A full copy of a Zentyal server with all its modules, but without user data will be around 300MB.





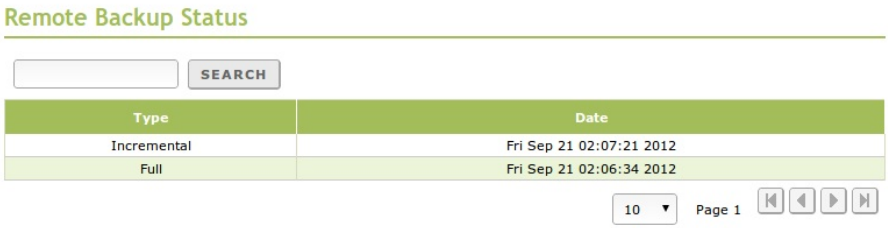
Exclude path	/var/cache
Exclude path	/var/spool
Exclude path	/tmp
Exclude path	/media
Exclude path	/mnt
Exclude path	/sys
Exclude path	/proc
Exclude path	/dev

10 Page 1

Inclusion and Exclusion list

Checking the status of the backups

You can check the backups status in the *Remote Backup Status* section. Within this table, you can see the type of backup; full or incremental and the execution date.



Available backup list

Restore files

There are two ways of restoring a file. Depending on the file size or the directory you want to restore.

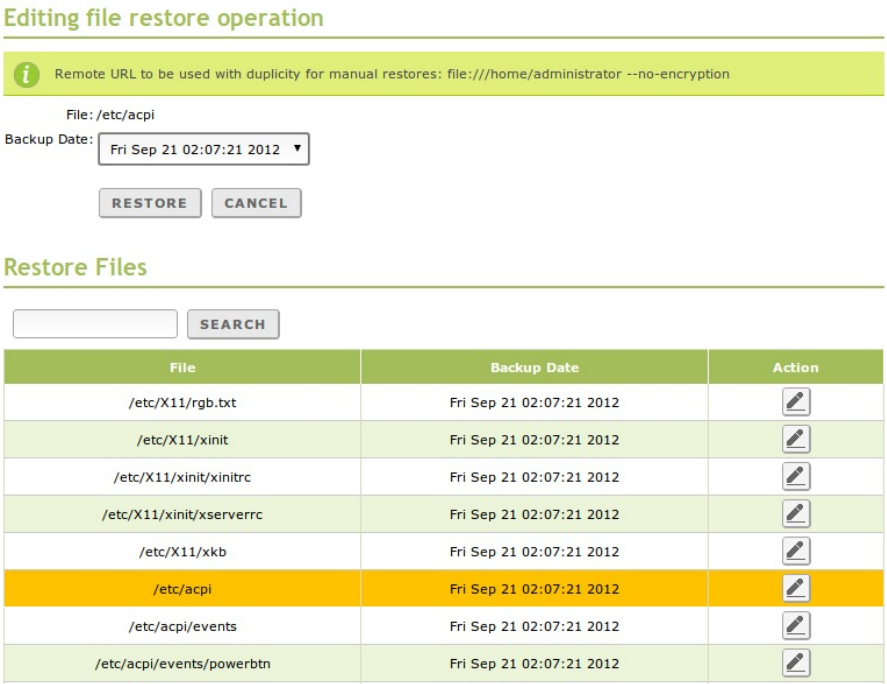
It is possible to restore files directly from Zentyal server's control panel. In the *System* ▸ *Backup* ▸ *Restore files* section you have access to the list of all the files and directories contained in the remote backup, and the dates of the different versions you can restore.

If the path to restore is a directory, all its contents will be restored, including sub-directories.

The file will be restored with its contents on the selected date, if the file is not present in the backup that day. The version found in the former backups will be restored. If there is no copy of the file in any of the versions, you will be notified with an error message.

Warning: The files shown in the interface are the ones that are present in the last backup. The files that are stored in former copies, but not in the last one, are not shown, but they can be restored using the command line.

You can use this method with small files. For big files, the process is time consuming and you can not use the Zentyal web interface while the operation is being made. You have to be especially careful with the type of file you are restoring. Normally, it will be safe to restore data files that are not being used by applications at the current time. These data files are located in the directory `/home/samba`. On the other hand, restoring system file of directories like `/lib`, `/var` or `/usr` while the system is running can be very dangerous. **Don't** do this unless you are really sure of what you are doing.



Restore a file

Restore services

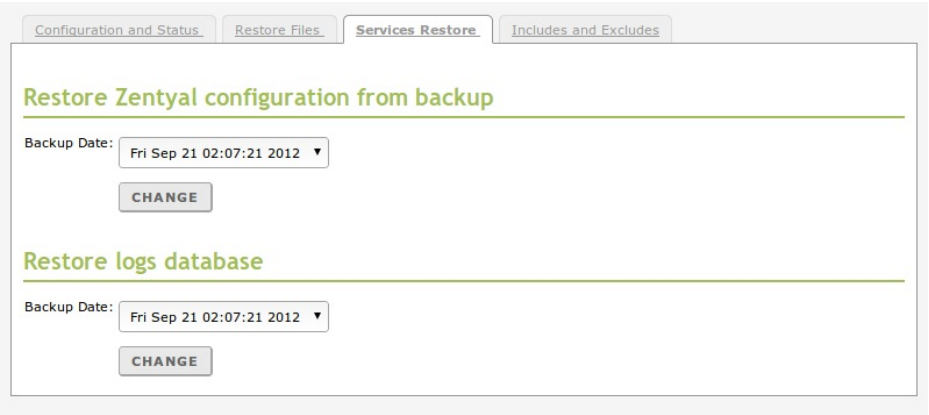
Apart from the files, additional data is stored to allow the direct restoration of some services. This data includes:

- Zentyal configuration backup
- backup of the registers database of Zentyal

In the tab *Services Restore* both can be restored for a given date.

The security copy of Zentyal configuration contains the configuration of all the modules that have been enabled at least once, all the LDAP data and any other additional files needed by the modules to function properly.

You have to be careful when restoring Zentyal configuration because all the current configuration and LDAP data will be replaced. Nevertheless, for the case of configuration not stored in LDAP, you have to click “Save changes” to make this effective.



Restoring services

Copyright 2004-2012 Zentyal S.L.

Zentyal Unified Communications

In this section you will see the different communication services integrated in Zentyal, which enable centralised management of an organisation's communications, and allow users to work with all them using the same password.

To start with, the e-mail service is described. It allows quick and easy integration with the user's e-mail clients, offering also spam and viruses prevention.

Since email became popular, it has suffered from unwanted mail, sent in bulk. This type of mail is often used to deceive the recipient in order to obtain money fraudulently, or simply unwanted advertising. You will also see how to filter incoming and outgoing e-mail within your network and to avoid both the reception of unwanted emails and block outgoing mail from any potentially compromised computer of your network.

The corporate instant messaging service, based on *Jabber/XMPP*, is also described. This module provides an internal IM service without having to rely on external companies or an Internet connection and ensures that conversations will be kept confidential, preventing data being passed through third parties. This service provides conference rooms. It allows, through the use of any of the many available clients, to have synchronous written communication in the organisation.

It is becoming increasingly important to use a system to help coordinate the daily work of employees within an organisation. For this, Zentyal

integrates a groupware tool which allows users to share information such as calendars, tasks, addresses and so forth.

Finally, you will see an introduction to voice over IP (or *VoIP*), this service offers each user an extension to easily make calls or participate in conferences. Additionally, through an external provider, Zentyal can be configured to connect to the traditional telephone network and make phone calls to any country in the world at significantly reduced rates.

Copyright 2004-2012 Zentyal S.L.

Electronic Mail Service (SMTP/POP3-IMAP4)

Zentyal uses **Postfix** [6] as a MTA. For the MDA (POP3, IMAP), it uses **Dovecot** [7]. Both come with support for secure communication over SSL. To fetch mail from external accounts, Zentyal uses **Fetchmail** [8] .

[6] **Postfix** *The Postfix Home Page* http://www.postfix.org .

[7] **Dovecot** *Secure IMAP and POP3 Server* http://www.dovecot.org .

[8] http://fetchmail.berlios.de/

SMTP/POP3-IMAP4 server configuration with Zentyal

Receiving and relaying mail

To understand the mail system configuration, the difference between receiving mail and relaying mail must be clear.

Reception occurs when the server accepts a mail message which recipients contain an account that belongs to any of its virtual mail domains. Mail can be received from any client that is able to connect to the server.

Relay occurs when the mail server receives a message which recipients do not belong to any of its managed virtual mail domains, thus requiring forwarding of the message to other servers. Mail relay is restricted, otherwise *spammers* could use the server to send spam all

over the Internet.

Zentyal allows mail relay in two cases:

1. Authenticated users.
2. A source address that belongs to a network object which has a **allowed relay** policy enabled.

General configuration

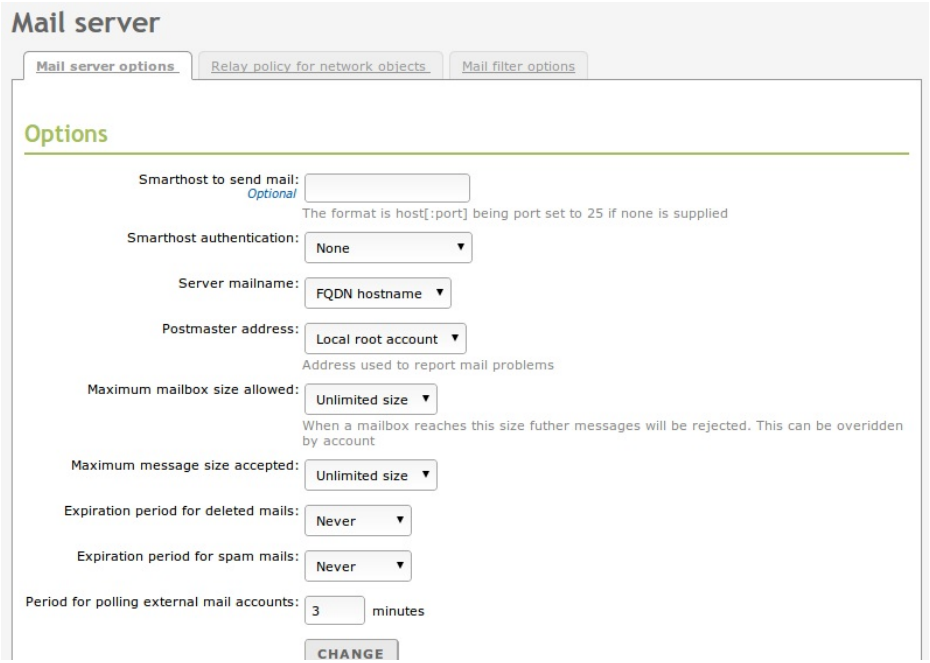
Accessing *Mail* ▸ *General* ▸ *Mail server options* ▸ *Options*, you can configure the general settings for the mail service:

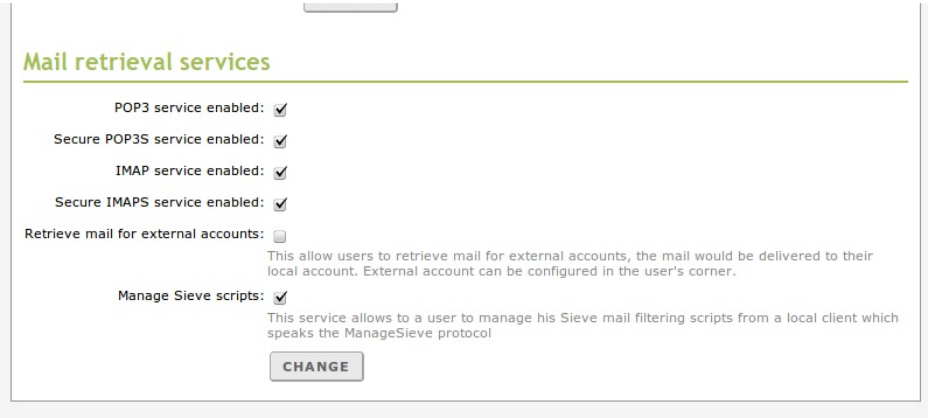
TLS for SMTP server:

This forces the clients to connect to the mail server using TLS encryption, thus avoiding eavesdropping.

Require authentication:

This setting enables the use of authentication. A user must provide an e-mail address and a password to identify; once authenticated, the user can relay mail through the server. An account alias can not be used to authenticate.




Mail retrieval services
POP3 service enabled:
Secure POP3S service enabled:
IMAP service enabled:
Secure IMAPS service enabled:
Retrieve mail for external accounts:
This allow users to retrieve mail for external accounts, the mail would be delivered to their local account. External account can be configured in the user's corner.
Manage Sieve scripts:
This service allows to a user to manage his Sieve mail filtering scripts from a local client which speaks the ManageSieve protocol
CHANGE

General Mail configuration

Smarthost to send mail:

If this option is set, Zentyal will not send its messages directly, but each received e-mail will be forwarded to the *smarthost* without keeping a copy. In this case, Zentyal is an intermediary between the user who sends the e-mail and the server that actually sends the message.

Here you can set the domain name or IP address of the smarthost. You could also specify a port appending the text *: [port_number]* after the address. The default port is the standard SMTP port, 25.

Smarthost authentication:

This sets whether the smarthost requires authentication using a user and password pair, or not.

Server mailname:

This sets the visible mail name of the system; it will be used by the mail server as the local address of the system.

Postmaster address:

The postmaster address by default is an alias of the root user, but it could be set to any account; either belonging to any of the managed virtual mail domains or not.

This account is intended to be a standard way to reach the administrator of the mail server. Automatically-generated

notification mails will typically use *postmaster* as reply address.

Maximum mailbox size allowed:

Using this option you could indicate a maximum size in MB for any user's mailboxes. All mail that exceeds the limit will be rejected and the sender will receive a notification. This setting could be overridden for any user in the *Users and Groups* ▸ *Users* page.

Maximum message size accepted:

It indicates, if necessary, the maximum message size accepted by the smarthost in MB. This is enforced regardless of any user mailbox size limit.

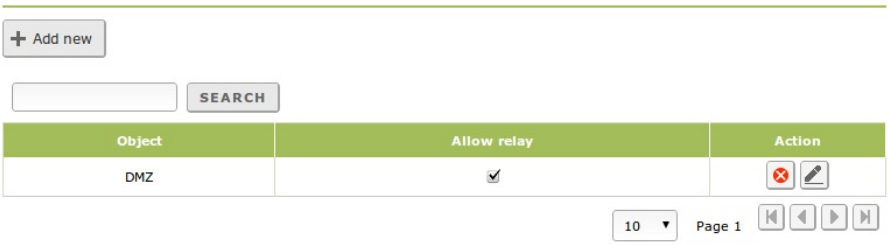
Expiration period for deleted mails:

If you enable this option, those mail messages that are in the users' trash folder will be deleted when their dates exceeds the established limit.

Expiration period for spam mails:

This option applies, in the same way as the previous option, but refers to the users' spam folder.

In addition to this, Zentyal can be configured to relay mail without authentication from some network addresses. To do this, you can add relay policies for Zentyal network objects through *Mail* ▸ *General* ▸ *Relay policy for network objects*. The policies are based on the source mail client IP address. If relay is allowed by an object, then each object member can relay e-mails through Zentyal.

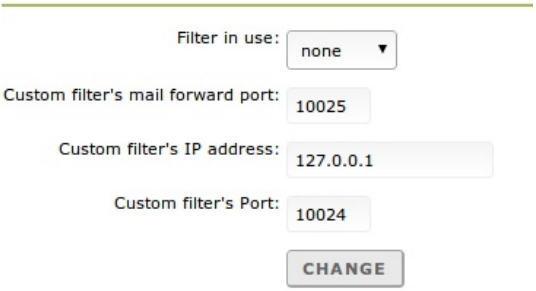


Relay policy for network objects

Warning: Be careful when using an *Open Relay* policy, i.e. forwarding e-mail from everywhere, your mail server will probably become a spam source.

Finally, the mail server can be configured to use a content filter for messages [10]. To do so, the filter server must receive the message from a specific port and send the result back to another port where the mail server is bound to listen to the response. You can choose a custom mailfilter or use Zentyal as a mail filter through *Mail ▸ General ▸ Mail filter options*. If the **mailfilter** module is installed and enabled, it will be used by default.

[10] This topic is deeply explained in the *Mail filter* section.



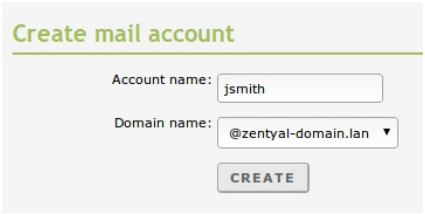
Mailfilter options

E-mail account creation through virtual domains

To set up an e-mail account, a virtual domain and a user are required. You can create as many virtual domains as you want from *Mail ▸ Virtual Domains*. They provide the *domain name* for e-mail accounts of Zentyal users. Moreover, it is possible to set *aliases* for a virtual domain, so that sending an e-mail to a particular virtual domain or to any of its aliases becomes transparent.

Virtual mail domains

In order to set up e-mail accounts, you have to follow the same rules used when configuring filesharing. You can select the main virtual domain for the user from *Users and Groups* ▸ *Users* ▸ *Edit Users* ▸ *Create mail account*. You can create aliases if you want to set more than a single e-mail address for a user. Regardless of whether aliases have been used, the e-mail messages are kept just once in a mailbox. However, it is not possible to use the alias to authenticate, you always have to use the real account.



Mail settings for a user

Note that you can decide whether an e-mail account should be created by default when a new user is added to Zentyal. You can change this behaviour in *Users and Groups* ▸ *Default User Template* ▸ *Mail Account*.

Likewise, you can set up *aliases* for user groups. Messages received by these aliases are sent to every user of the group with an e-mail account. Group aliases are created through *Users and Groups* ▸ *Groups* ▸ *Create alias mail account to group*. The group aliases are only available when, at least, one user of the group has an e-mail account.

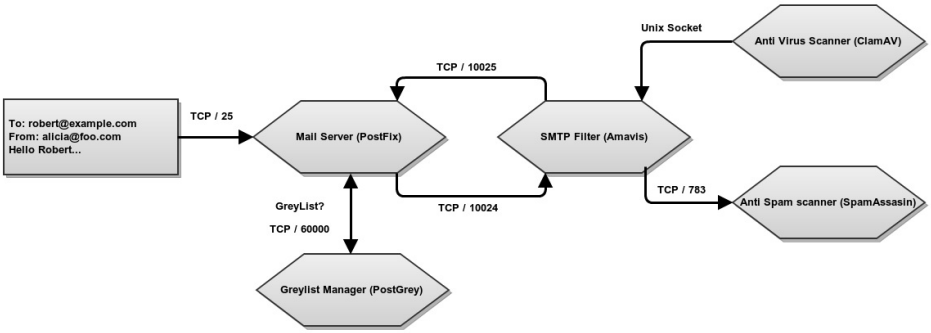
You can define an alias to an external account as well, that is, mail accounts associated to domains not managed by your server. The mail sent to that alias will be forwarded to the external account. These kind of aliases are set on a virtual domain basis and do not require an e-mail account. They can be set in *Mail* ▸ *Virtual Domains* ▸ *External accounts aliases*.

Copyright 2004-2012 Zentyal S.L.

Mail filter

Mail filter schema in Zentyal

Zentyal offers a powerful and flexible mail filter to defend your network and users from these threats.



Mail filter schema in Zentyal

In the figure, you can see the different steps an e-mail passes through before being tagged as valid or not. First, the email server sends it to the greylisting policies manager and if considered as potential spam, the system requests that the email is forwarded to the source server. If the email passes through this filter, it will move to the mail filter. This will use a statistical filter to check a series of email features to discover whether it contains virus or is junk mail. If the email passes through all the filters, it is considered valid and it is sent to the recipient or stored on the server's mailbox.

In this section the details of each filter and how to configure them in Zentyal will be explained step by step.

Grey list

The **grey lists** [1] exploit the expected performance of mail servers dedicated to *spam*. The behaviour is matched and all mail from the servers is discarded or not, hindering the spamming process.

These servers are optimised to send as many emails as possible in minimal time. For this, messages are auto-generated and sent without caring if they are received. When you have a **grey list** system, the emails considered as potential *spam* are rejected and the mail server is asked to send the email again. If the server is actually a *spammer* server, it probably doesn't have the necessary tools to manage this request and

it probably doesn't have the necessary tools to manage this request and therefore the email will never reach the recipient. On the contrary, if the email was legitimate, the sending server will simply re-send mail.

[1] Zentyal uses **postgrey** (http://postgrey.schweikert.ch/) as a **postfix** policy manager.

The Zentyal strategy is to pretend to be out of service. When a new server sends an email, Zentyal responds "*I am temporarily out of service*" during the first 300 seconds [2]. If the sending server complies with the request, it will re-send the email after this time and Zentyal will mark it as a valid server.

Zentyal does not include email sent from internal networks on the gray list, or from objects with an allowed email relay policy or from addresses that are in the *antispam* whitelist.

[2] Actually the mail server responds "Greylisted", i.e. moved to the grey list and pending to allow or disallow the mailing once the configured time has passed.

The *Grey list* can be configured via *Mail* ▸ *Grey list* with the following values:

Greylist configuration
Enabled:
Greylist duration (seconds):
300
During this interval, the mail sender is deferred
Retry window (hours):
48
Time that mail sender has to retry to be added before it will be greylisted again
Entries time to live (days):
35
Period till unseen entries will be deleted
CHANGE

Grey list configuration

Enabled:

Click to enable *greylisting*.

Grey list duration (seconds):

Seconds the sending server must wait before re-sending the email.

Retry window (hours):

Time in hours in which the sending server can send mail. If the server receives any mail during this time, this server will go to the grey list. In a grey list the server can send all the emails it wishes with no time restrictions.

Entry time-to-live (days):

Days the data of the evaluated servers will be stored in the grey list. After the configured days, when the server sends email again, it must go through the *greylisting* process described above.

Content filtering system

The mail content filtering is processed by the **antivirus** and **spam** detectors. To carry out this task, Zentyal uses an interface between the MTA and these applications. Therefore, the **amavisd-new** [3] application is used to ensure that the email is not spam and it does not contain viruses.

In addition, *amavisd* carries out the following checks:

- File extension and black and white lists.
- Mail filtering of emails with malformed headers.

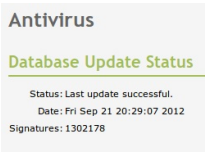
[3] **Amavisd-new**: http://www.ijs.si/software/amavisd/

Antivirus

Zentyal uses the **ClamAV** [4] antivirus, an antivirus toolkit especially designed to scan email attachments in a MTA. **ClamAV** uses a database updater that allows the programmed updates and digital signatures to be updated via the **freshclam** program. Furthermore, the *antivirus* is capable of native scanning of a number of file formats, such as Zip, BinHex, PDF and so on.

[4] Clam Antivirus: http://www.clamav.net/

In *Antivirus* you can check if the system's *antivirus* is installed and updated.



Antivirus message

You can update it from *Software Management*, as you will see in *Software updates*.

It is optional to install the antivirus module, but if you do install it, you can see that it integrates several other Zentyal modules. This integration increases the security of the configuration options of different services, such as the SMTP filter, HTTP *proxy* or file sharing.

Antispam

The *antispam* filter gives each email a *spam* score and if the email reaches the *spam* threshold it is considered junk mail. If not, it is considered as legitimate email. The latter kind of email is often called *ham*.

The spam scanner uses the following techniques to assign scores:

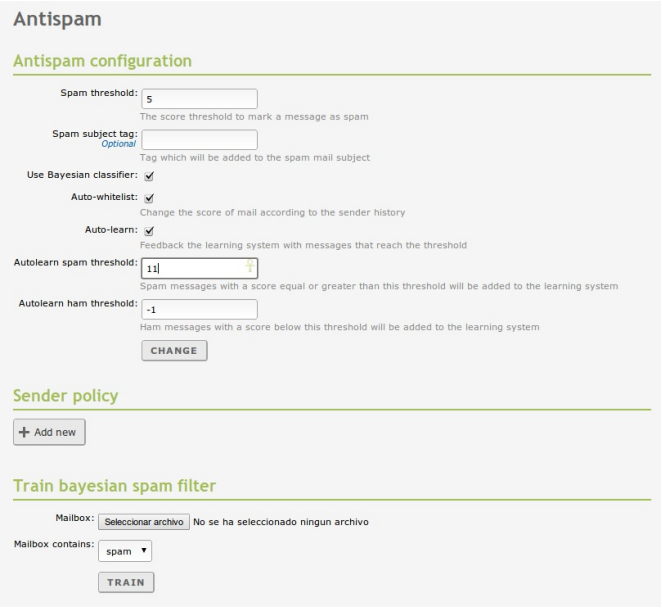
- Blacklists published via DNS (*DNSBL*).
- URI blacklists that trac *antispam websites*.
- Filters based on the message *checksum*, checking emails that are identical, but with some few changes.
- Bayesian filter, a statistical algorithm that learns from its past mistakes when classifying an email as *spam* or *ham*.
- Static rules.
- Other. [5]

Zentyal uses **Spamassassin** [6] as *spam* detector.

[5] You can find a long list of *antispam* techniques at http://en.wikipedia.org/wiki/Anti-spam_techniques_(e-mail)

[6] The Powerful #1 Open-Source Spam Filter http://spamassassin.apache.org .

The general configuration of the filter is done from *Mail filter* ▸ *Antispam*:


Antispam
Antispam configuration
Spam threshold:
5
The score threshold to mark a message as spam
Spam subject tag:
Optional
Tag which will be added to the spam mail subject
Use Bayesian classifier:
Auto-whitelist:
Change the score of mail according to the sender history
Auto-learn:
Feedback the learning system with messages that reach the threshold
Autolearn spam threshold:
11
Spam messages with a score equal or greater than this threshold will be added to the learning system
Autolearn ham threshold:
-1
Ham messages with a score below this threshold will be added to the learning system
CHANGE
Sender policy
Add new
Train bayesian spam filter
Mailbox:
Seleccionar archivo
No se ha seleccionado ningun archivo
Mailbox contains:
spam
TRAIN

Antispam configuration

Spam threshold:

Mail will be considered spam if the score is above this value.

Spam subject tag:

Tag to add to the mail subject in case it is spam.

Use Bayesian classifier:

If marked, Bayesian filter will be used. Otherwise it will be ignored

Auto-whitelist:

Considers the account history of the sending server when giving the score to the message; if the sender has sent plenty of *ham* emails, it is highly probable that the next email will be *ham* and not *spam*.

Auto-learn:

If marked, the filter will learn from the received messages, which score passes the auto-learn thresholds.

Autolearn spam threshold:

The filter will learn that email is *spam* if the score is above this value. You should not set a low value, since it may cause false positives. The value must be greater than the spam threshold.

Autolearn ham threshold:

Filter will learn if the email is *ham* if the score is below this value. You should not set a high value, since it may cause false negatives. The value must be less than 0.

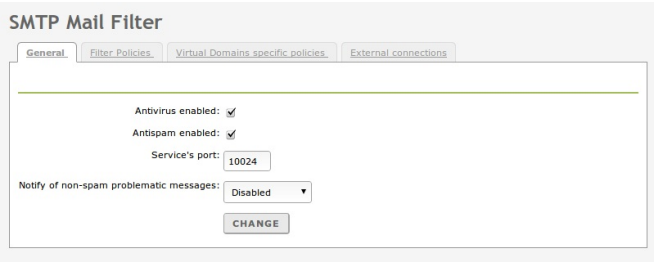
From *Sender Policy* you can configure senders whose emails are always accepted (*whitelist*), always marked as spam (*blacklist*) or always processed by the antispam filter (*process*). If a sender is not listed here, the default behaviour will be *process*.

From *Train Bayesian spam filter* you can train the Bayesian filter by sending it a mailbox in *Mbox* [7] format, containing only *spam* or *ham*. You can find many sample files from the Internet to train the Bayesian filter, but usually you get more accurate results if you use email received from the sites you need to protect. The more trained the filter is, the better results you get when testing if a message is junk or not.

[7] *Mbox* and *maildir* are email storage formats, independent of the the used email client. For Mbox, all the emails are stored in a single file, whilst maildir organises emails into separate files within a directory.

SMTP mail filter

From *Mail filter* ▸ *SMTP mail filter* you can configure the behaviour of the described filters, when Zentyal receives mail by SMTP. From *General* you can configure the general behaviour of all incoming mail:



General parameters for the SMTP filter

Enabled:

Check to enable SMTP filter.

Antivirus enabled:

Check to ensure the filter searches for viruses.

Antispam enabled:

Check to ensure the filter searches for *spam*.

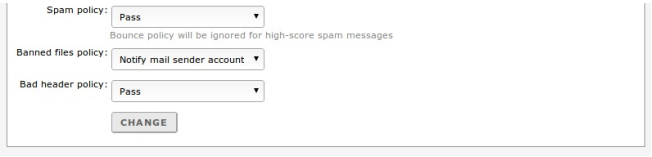
Service's port:

Port to be used by the SMTP filter.

Notify of non-spam problematic messages:

You can send notifications to a mailbox when you receive problematic emails that aren't spam, for example, emails infected by a virus.

From *Filter policies* you can configure how the filter must act with different types of emails.



SMTP filter policies

You can perform following actions with problematic emails:

Pass:

Do nothing, let the email reach its recipient. Nevertheless, in some cases like *viruses*, the mail server will add a warning to the email subject.

Notify mail server account:

Discard the message before it reaches the recipient, notifying the original sender account.

Notify sender server:

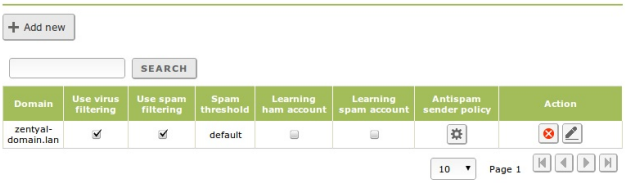
Discard the message before it reaches the recipient, notifying the server of the sender account, it's very common that, the server notifies its user in turn about this with a *Undelivered Mail Returned to Sender* message.

Drop silently

Discard the message before it reaches the recipient, without notifying the sender or his/her server.

From *Virtual domains* you can configure the behaviour of the filter for virtual domains of the email server. These settings override the previously defined default settings.

To customise the configuration of a virtual domain of the email, click on *Add new*.



Filter parameters per virtual domain of the mail

The parameters that can be overridden are the following:

Domain:

Virtual domain you want to customise. Those configured in *Mail* ▸ *Virtual domain* are available.

Use virus / spam filtering:

If enabled, the email received in this domain will be filtered in search of viruses or *spam*

Spam threshold:

You can use the default score for spam or custom value.

Ham / spam learning account:

If enabled, *ham@domain* and *spam@domain* accounts will be

created. The users can send emails to these accounts and train the filter. All the email sent to *ham@domain* will be recorded as not *spam* the email sent to *spam@domain* will be recorded as *spam*.

Once you have added the domain, you can add addresses to your whitelist, blacklist or force the processing from *Antispam policy for senders*.

Copyright 2004-2012 Zentyal S.L.

Webmail service

Zentyal integrates **Roundcube** to implement a webmail service [1]. Roundcube is developed with the latest web technologies, offering a far superior user experience compared to traditional webmail clients.

[1] http://roundcube.net/

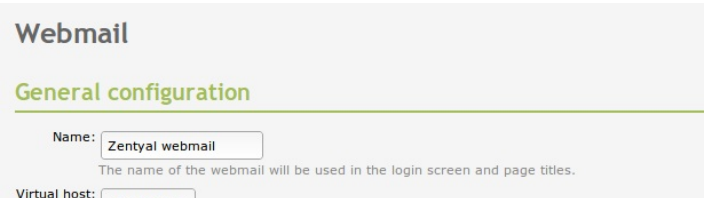
Configuring a webmail in Zentyal

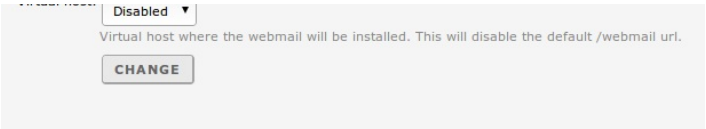
The webmail service is enabled in the same way as any other Zentyal service. However, the e-mail module must be configured to use either IMAP, IMAPS or both and the webserver module must be enabled. Without this configuration, webmail will refuse to work.

The e-mail configuration in Zentyal is explained in depth in the *Electronic Mail Service (SMTP/POP3-IMAP4)* section and the webserver module is explained in the *Web publication service (HTTP)* section .

Webmail options

You can access the settings by clicking in the *Webmail* section in the left menu. Here you can establish the title that will be used by webmail to identify itself. This title will be shown on the login screen and in the HTML page titles.



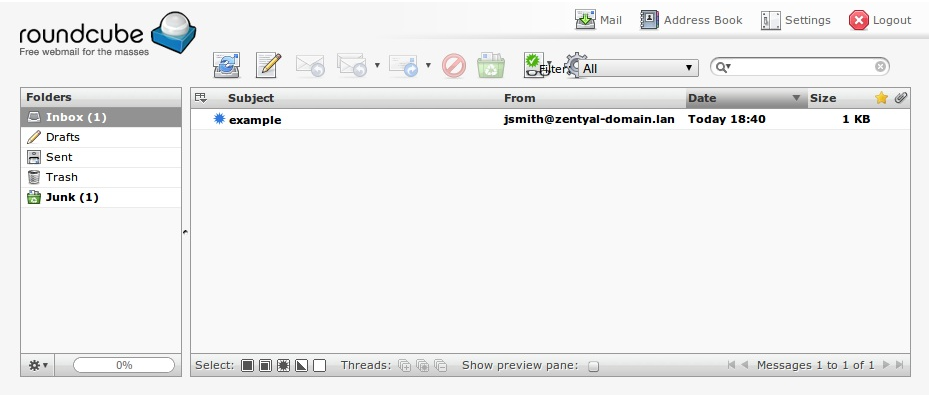


General Webmail settings

Login to webmail

To be able to log into the webmail interface, HTTP traffic must be allowed by the firewall from the source address used. The webmail login screen is available at *http://[Zentyal's address]/webmail* using the browser. Then the user has to enter his/her e-mail address and password. Only the real e-mail addresses are accepted for login, not aliases.

Webmail login



Example of a mail received using webmail

SIEVE filters

The webmail software also includes an interface to manage SIEVE filters. This feature is only available if the *ManageSIEVE* protocol is enabled in the e-mail service. Check out *Sieve scripts and ManageSieve protocol* section for more information.

Copyright 2004-2012 Zentyal S.L.

Groupware service

Zentyal integrates Zarafa [1] as a complete solution for groupware environment aiming to offer an alternative to Microsoft Exchange.

[1] http://www.zarafa.com/

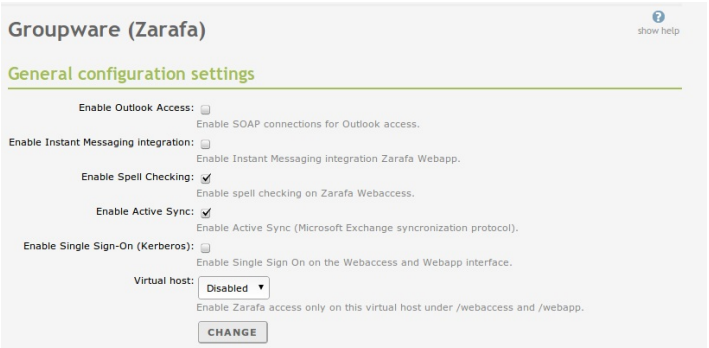
Configuration of a groupware server (Zarafa) with Zentyal

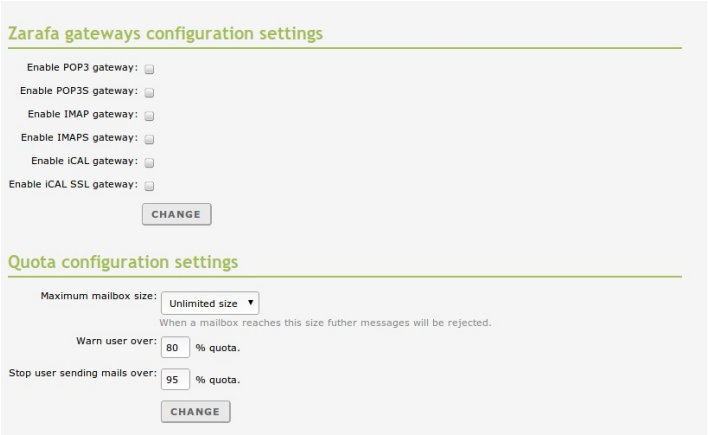
General configuration

In order to use Zarafa, you must start with a mail server configured as explained in *Electronic Mail Service (SMTP/POP3-IMAP4)*. In this scenario, you assign any number of the existing virtual domains to the *groupware* module and, from that moment on, the mail of those domains will be stored in Zarafa and not in the server you were using previously. The mail sent to the other virtual domains will continue to be stored in the same way.

This *groupware* module integrates with the existing mail module so that the users can consider themselves associated with a *quota* and use a Zarafa account.

You can access the configuration in *Groupware* ▸ *General* where the following parameters can be set:


Groupware (Zarafa)
show help
General configuration settings
Enable Outlook Access:
Enable SOAP connections for Outlook access.
Enable Instant Messaging integration:
Enable Instant Messaging integration Zarafa Webapp.
Enable Spell Checking:
Enable spell checking on Zarafa Webaccess.
Enable Active Sync:
Enable Active Sync (Microsoft Exchange syncronization protocol).
Enable Single Sign-On (Kerberos):
Enable Single Sign On on the Webaccess and Webapp interface.
Virtual host:
Disabled
Enable Zarafa access only on this virtual host under /webaccess and /webapp.
CHANGE



Configuration of groupware (Zarafa)

Enable Outlook access:

In case you want to integrate the Zarafa platform and all its groupware services (calendars, tasks, contacts) with a Microsoft Outlook client, you will need to enable this option, and also, to install the Zarafa plug-in in the Outlook client [4]. Free version support three clients, but you can buy additional licenses [5].

Enable Instant Messaging integration:

If you have the *Jabber* module installed and enabled, you will be able to use the chat windows integrated in Zarafa's web interface.

Enable spell checking:

Enable this option to check your spelling while you type an e-mail using the Zentyal web interface.

Enable ActiveSync:

Enable the support for ActiveSync mobile devices for synchronizing email, contacts, calendars and tasks. For more information, see the list of supported devices [6] .

Enable Single Sign-On (Kerberos):

Use Kerberos to automatically authenticate the user, similar to the equivalent option for GSSAPI/mail.

Virtual host:

The default installation allows access to the Zarafa web interface at http://ip_address/webaccess and http://ip_address/webapp for the new interface, you can also use the web server virtual domains to choose your own URL.

To provide users with POP3, POP3 on SSL, IMAP or IMAP on SSL access to their mailboxes, select the corresponding *Zarafa Gateways*. Keep in mind that if any of these services is already enabled in the mail module, it can not be enabled here. Also the *Zarafa Gateways* can

module, it can not be enabled here. Also the *Zarafa Gateways* can only authenticate users with a Zarafa account and not users with only an email account.

Finally, you can define the email **quota**, i.e. the maximum mailbox size each user can have. The user will receive a notification email when the specified percentage in the first limit is exceeded and if the second limit is exceeded, the user will not be allowed to continue sending emails until they have freed up some space. When a user reaches the maximum *quota*, emails sent to this user will be rejected.

You can configure the mail domains that will be managed by Zarafa going to *Groupware* ▸ *Virtual Mail Domains*

Configuration of a Zarafa account

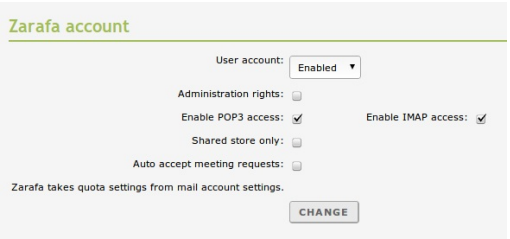
As mentioned earlier, besides an email account, each user should have a Zarafa account. Furthermore, the quota defined in the mail module for each user will be applied to Zarafa, this can be unlimited globally defined or specifically set per user.

[4] http://doc.zarafa.com/7.1/User_Manual/en-US/html/_configure_outlook.html#_installation_of_the_outlook_client

[5] https://store.zentyal.com

User configuration

Accessing the configuration of your users you can modify the following Zarafa parameters:



Per-user Zarafa parameters

User account

Whether this user has Zarafa access enabled or not

Administration rights

Administration rights

The administrator user will be able to manage all the permissions of the Zarafa platform.

Enable access

The protocols offered here will depend on your specific configuration, you can set the protocols that will be available for this user.

Shared store only

This option is used when you have an account that is really a shared resource, and nobody logins using it, for example, a calendar shared between several people.

Auto accept meeting requests

Add the requests to our calendar without confirming with the user, the user will be notified of this event via email.

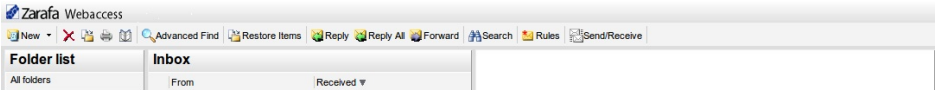
Until now, mail users were authenticated by the name of their email account, for example *bob@home.lan*. Zarafa web interface, or its gateways, expects users to be identified by their username, as *bob* in the previous example. Configuration for delivery through SMTP does not change.

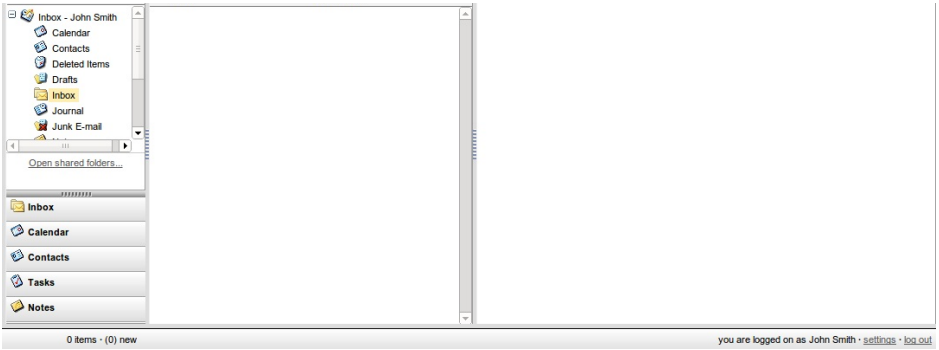
Zarafa basic use cases

Once you have configured your Zarafa server and have authorized users, you can access it through the configured *Virtual Host*

Zarafa login screen

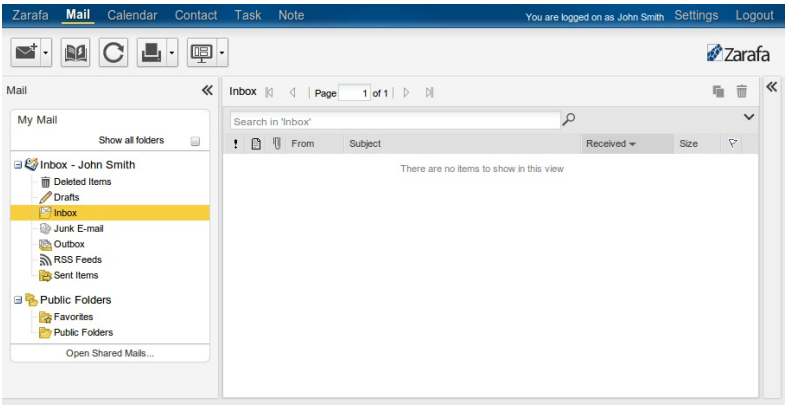
After login in you can see the main Zarafa page, showing the email interface and different tabs to access the *Calendars*, *Contacts*, *Tasks* and *Notes*





Zarafa main page

Zarafa also sports a renew version of their interface, *WebApp*

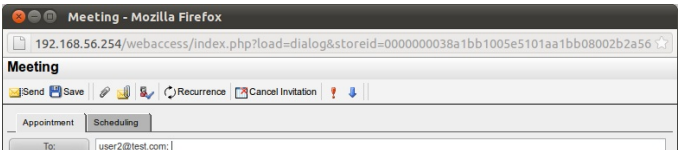


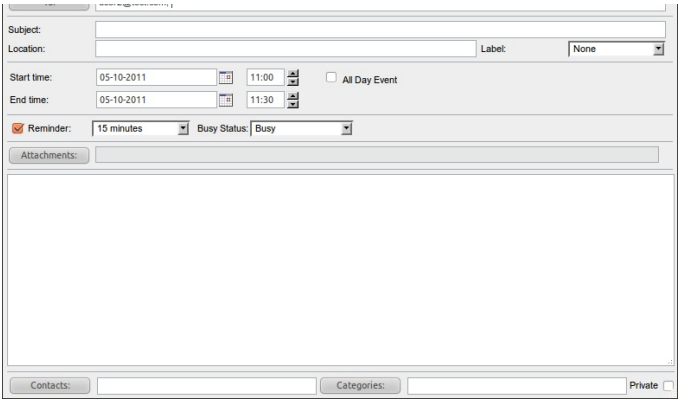
WebApp version of the Zarafa

Shared calendars

Suppose a very common use case where you want to schedule an event between several users, for example a meeting

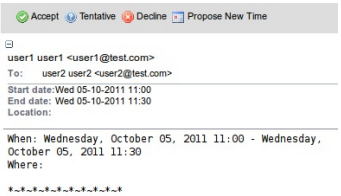
To do this, you should go to the *Calendar* tab and create an event, simply by double clicking in the desired date and time. As you can see, there are many parameters you can configure like duration, reminders, attached files, schedule, etc. During the event configuration or editing it later, you can invite other users from the *Invite attendees* tab. You only need to fill his/her mail address and click on *Send*.





Sending an event invitation

The recipient will receive a custom mail with the event specification, including a submenu that allows him/her to accept or decline the invitation, or even propose a new time.



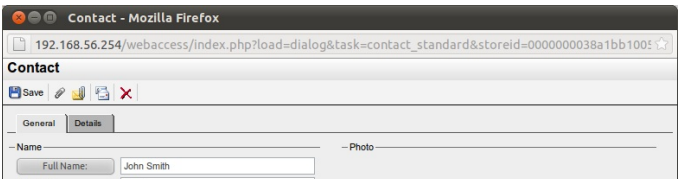
Receiving a mail invitation

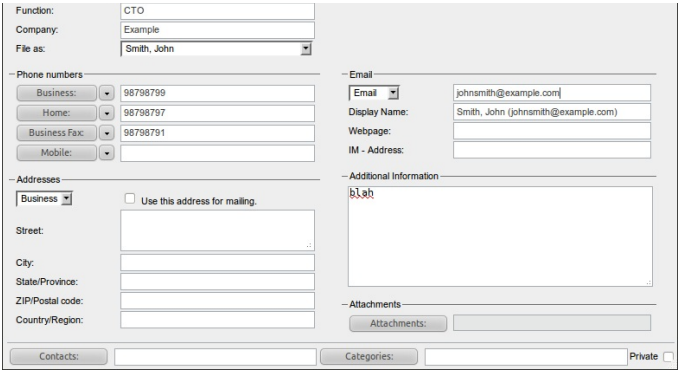
Whether you accept or decline the event invitation, you can notify the sender back and include an explanatory text. In case you accept the event, it will be automatically added to your personal calendar.

Shared contacts

Another common use case is to share your business contact to have a centralized and organized point to retrieve this information.

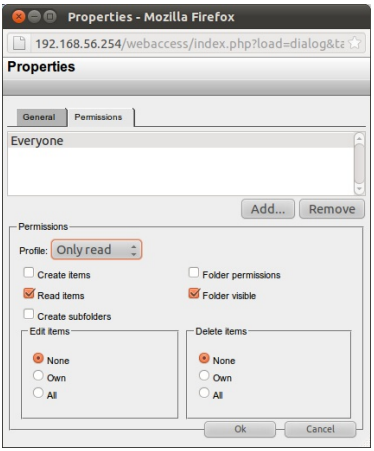
First of all, you can create a contact through the *New* ▸ *Contact* menu. As you can see the form is quite complete: you can include several phone numbers, email and addresses, portrait, attached files, department, role, etc.





Creating a new contact

Once you have created the contact, you can share the folder by right clicking over the folder and accessing *Properties*, in this submenu, you access the tab *Permissions* and click on the *Add* button. Add the user 'Everyone' (access for all Zarafa users) and choose the *Profile Only read*. After this just *Accept*.



Sharing a contact with other Zarafa users

After this, you can access with other user and click on the *Open shared folders* link that you can see in the main Zarafa webpage. In the pop-up window, fill in the *Name* with the email address of the user that has shared the contacts and in *Folder type* choose *Contacts*. A new folder will appear in you main window, where you can see the shared contacts.

For more information about Zarafa, see the User Manual [7]. For administrators that require a deeper understanding of the application, reading of the Administration Manual [8] is recommended.

[6] http://www.zarafa.com/wiki/index.php/Z-Push_Mobile_Compatibility_List
[7] http://doc.zarafa.com/trunk/User_Manual/en-US/html/index.html
[8] http://doc.zarafa.com/trunk/Administrator_Manual/en-US/html/index.html

Copyright 2004-2012 Zentyal S.L.

Instant Messaging Service (Jabber/XMPP)

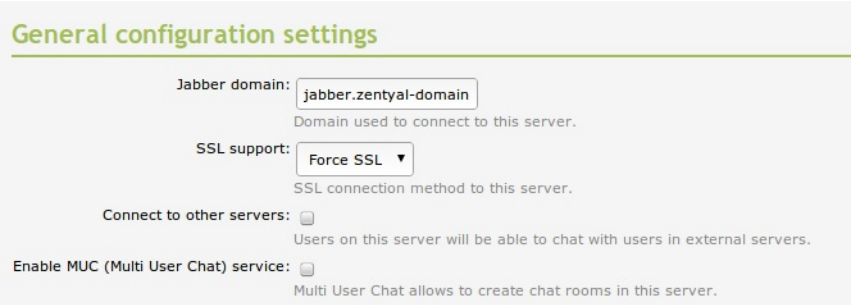
Zentyal uses Jabber/XMPP as its IM protocol and **jabberd2** [3] XMPP server, integrating network users with Jabber accounts.

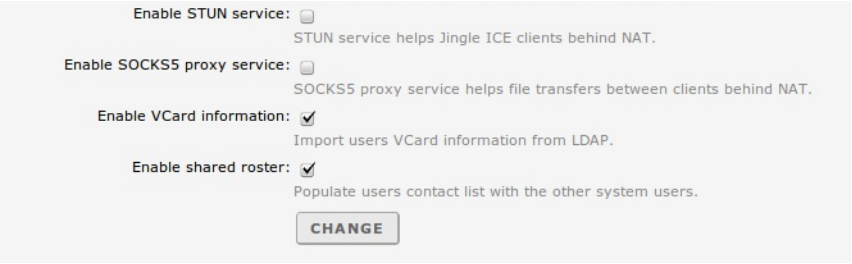
[3] http://www.ejabberd.im/

Configuring a Jabber/XMPP server with Zentyal

To configure the Jabber/XMPP server in Zentyal, first check the *Module Status* and that the *Users and Groups* module is enabled - Jabber depends on this. Then, mark the *Jabber* checkbox to enable the Jabber/XMPP Zentyal module.

To configure the service, go to *Jabber* in the left hand menu, and set the following parameters:


General configuration settings
Jabber domain:
jabber.zentyal-domain
Domain used to connect to this server.
SSL support:
Force SSL
SSL connection method to this server.
Connect to other servers:
Users on this server will be able to chat with users in external servers.
Enable MUC (Multi User Chat) service:
Multi User Chat allows to create chat rooms in this server.


Enable STUN service:
STUN service helps Jingle ICE clients behind NAT.
Enable SOCKS5 proxy service:
SOCKS5 proxy service helps file transfers between clients behind NAT.
Enable VCard information:
Import users VCard information from LDAP.
Enable shared roster:
Populate users contact list with the other system users.
CHANGE

General Jabber Configuration

Jabber Domain:

Used for specifying the domain name of the server. User accounts will be *user@domain*.

SSL Support:

It specifies whether the communications (authentication and chat messages) with the server are encrypted or plain text. You can disable it, make it mandatory or leave it as optional. If you set it as optional, this setting will be selected from the Jabber client.

Connect to other servers:

If you want to allow your users to contact other users on external servers, or the other way around, check this box. Otherwise, if you want a private server for your internal network, leave it unchecked.

Enable MUC (Multi User Chat):

Enables conference rooms (chat with more than two users).

Enable STUN service:

Service that implements a set of methods to stablish connections between clients that are located behind a NAT, for example video conferences using *Jingle*.

Enable SOCKS5 proxy service:

Proxy service for TCP connection, can allow the clients behind a NAT to send files.

Enable VCard information:

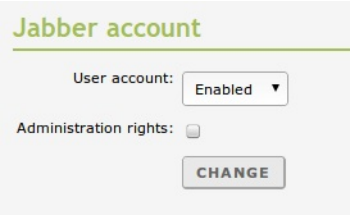
Manage the contact information, using the VCard format, this info could be also browsed and edited from the *Groupware* module

(Zarata).

Enable shared rosted:

Autocratically add all the users of this server as contacts of your list.

To create a Jabber/XMPP user account, go to *Users* ▸ *Add User* if you want to create a new user account, or to *Users* ▸ *Edit User* if you just want to enable the Jabber account for an existing user.



Setting up a Jabber account

As you can see, a section called *Jabber account* will appear, where you can select whether the account is enabled or disabled. Moreover, you can specify whether the user will have administrator privileges. Administrator privileges allow you to see which users are connected to the server, send them messages, set the message displayed when connecting (*MOTD*, Message Of The Day) and send a notice to all connected users (broadcast).

Copyright 2004-2012 Zentyal S.L.

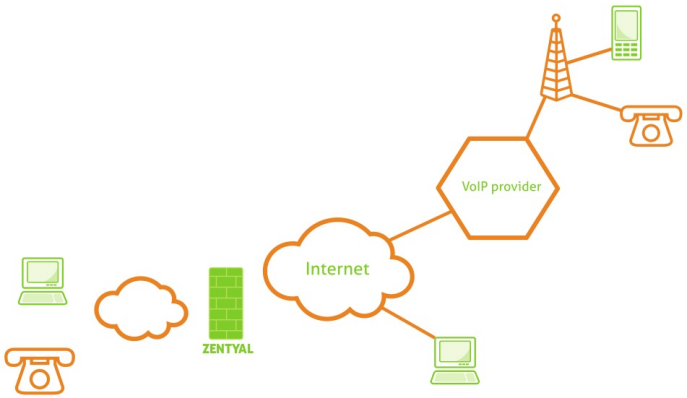
Voice over IP service

Zentyal uses **Asterisk** [6] to implement the VoIP module. *Asterisk* is a software only application that works on any commodity server, providing the features of a PBX (*Private Branch eXchange*) to connect multiple phones, using a VoIP provider or the analog telephone network. It also offers services such as voice mail, conferences, interactive voice responses and so on.

[6] http://en.wikipedia.org/wiki/Asterisk_(PBX)

VoIP server configuration with Zentyal

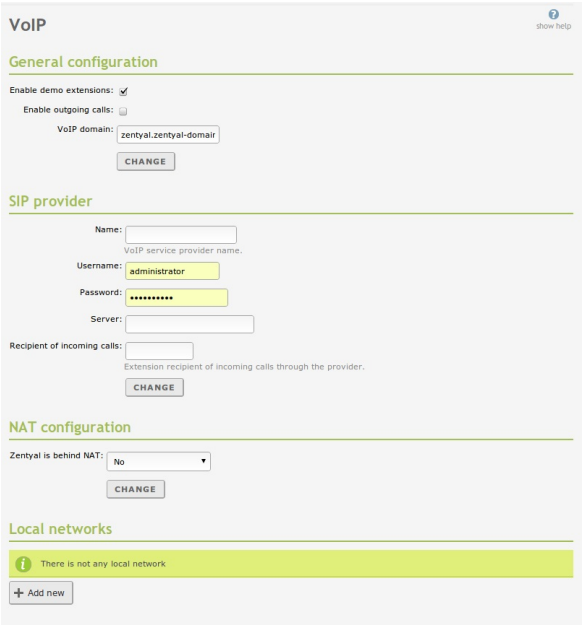
Zentyal VoIP module allows you to easily manage an *Asterisk* server with the users that already exist on the system's LDAP server, and to configure the most common features.



Basic diagram of how VoIP works

As usual, the module must be enabled first. Go to *Module Status* and select the *VoIP* checkbox. The *Users and groups* should be enabled

select the *VoIP* checkbox. The *Users and groups* should be enabled beforehand.



VoIP configuration window in Zentyal

To change the general configuration, go to *VoIP* ▸ *General*. Once there, the following general parameters should be configured:

Enable demo extensions:

Enables the extensions *4 and *6. If you call to the extension *4, you will be able to hear the waiting musing. Using the extension *6 you will have an *echo test* to give you an estimation of the latency in your calls.

Enable outgoing calls:

This enables outgoing calls through a SIP provider to call regular phones. To call through the SIP provider, add an additional zero before the number to call. For instance, to call Zentyal offices (+34 976733506 or 0034976733506) dial 00034976733506.

VoIP domain:

This is the domain assigned to the user addresses. For example, a user *user* with an extension 1122 can be called at user@domain.tld or at 1122@domain.tld.

In the *SIP provider* section, enter the credentials supplied by the SIP provider, so that Zentyal can route calls through it:

Name:

The identifier of the provider in Zentyal.

User name:

The user name used to log into the provider service.

Password:

The password to log into the provider service.

Server:

The provider server.

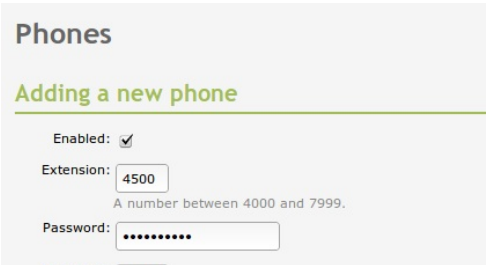
Recipient of incoming calls:

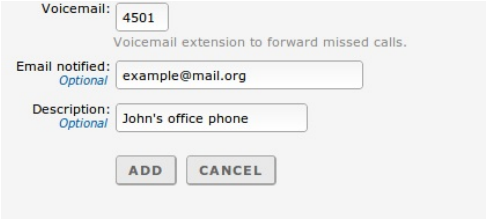
The internal extension that will receive the incoming calls to the provider account.

The *NAT configuration* section defines the network location of your Zentyal host. If it has a public IP address, the default option *Zentyal is behind NAT: No* is correct. If it has a private IP address, you must provide *Asterisk* with your *Internet* public IP address. If you have a fixed public address, select *Fixed IP address* and enter it; if the IP is dynamic, you must configure the dynamic DNS service (Dynamic DNS) available in *Network* ▸ *Dynamic DNS* (or configure it manually) and enter the domain name in *Dynamic hostname*.

In the *Local networks* section, you can add the local networks to which Zentyal has direct access without NAT, like VPN or network segments not configured from Zentyal, like a wireless network. This is required due to SIP behaviour in NAT environments.

To configure the authentication of the VoIP phones, go to *VoIP* ▸ *Phones*





Adding a VoIP phone

Enabled:

Whether this phone configuration is enabled.

Extension:

Extension to dial to reach this phone.

Password:

Needed to authenticate the phone against Zentyal, it will have to be configured in the phone itself as well.

Voicemail:

The device available through this extension will store the voicemail for this phone.

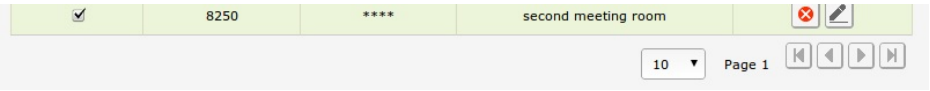
Email notified:

This email address will receive the voicemail messages as an attachment.

Description:

Description of the specific phone

You can access the conference configuration through *VoIP* ▸ *Meetings*. Here you can configure multiple conference rooms. These rooms *extension* should fit in the 8001-8999 range and optionally have an *access password*, an *administration password* and a *description*. These extensions can be accessed from any server by dialling extension@domain.tld.

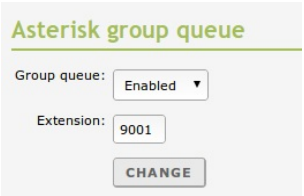


List of meetings

When you edit a user, you will be able to enable and disable this user's VoIP account and change his/her extension. Take into account that an extension can only be assigned to one user and no more, if you need to call more than one user from an extension, you must use queues.

Managing the VoIP per user

When editing a group, you can enable and disable group's queue. A queue is an extension and when a call is made to a queue, all the users who belong to this queue will receive the same call.



Managing the VoIP queues per group

Using Zentyal VoIP features

Call transferring

The **call transferring** feature is quite simple. While you are in a conversation, press `#` and then dial the extension where you need to transfer the current call. You can hang up afterwards as the call will be ringing on the called extension.

Call parking

Call parking works on the extension 700. Whilst you are in a conversation, press `#` to initiate a transfer, then dial 700. The extension the call has been parked to will be announced to the called person. The caller will listen to call hold music, if configured. You can hang up now. From a different phone or a different user, the called person or group will dial the announced extension and the parked user will receive a wake up, and the call can start.

On Zentyal, the call parking can hold up to 20 concurrent calls and the maximum time a call can be parked is 300 seconds.

Voice mail

Using the extension *1, you can check your voice mail. The user and password will be the extension assigned by Zentyal when creating the user. Changing the password inmediatly is recommended, you can do that from the *User Corner*. The application listening in this extension allows you to change the welcome message, hear the stored messages and delete them. This extension is only accessible by the users of your server, it will not accept incoming calls from other servers for security reasons.

Copyright 2004-2012 Zentyal S.L.

Zentyal Maintenance

Zentyal server is not just meant to configure network services, but it also offers a number of features to ease general server management and maintenance.

This section will explain the tools, such as service logs, included in Zentyal server that help to find out what has happened in your network and when, receive notifications for certain events or incidents, or carry out server monitoring. The available remote support tools are also described.

Besides these maintenance tools integrated in Zentyal server, the commercial editions offer a series of services that help to automate the server maintenance and management. These services are available through the remote monitoring and management platform called **Zentyal Remote**.

Copyright 2004-2012 Zentyal S.L.

Logs

Zentyal log queries

Zentyal provides an infrastructure that allows its modules to log all types of events that may be useful for the administrator. These **logs** are available through the Zentyal interface. Logs are stored in a database so making queries, reports and updates is easier and more efficient. The database manager used is **MySQL**.

You can also configure different dispatchers for the events so that the administrator can be notified in different ways (Email, Jabber or RSS [1]).

[1] **RSS** *Really Simple Syndication* is an XML format used mainly to publish frequently updated works http://www.rssboard.org/rss-specification/.

Zentyal offers logs for the following services:

- OpenVPN *Virtual private network (VPN) service with OpenVPN*
- SMTP Filter *Mail filter*
- Printers *Printers sharing service*
- Firewall *Firewall*
- DHCP *Network configuration service (DHCP)*
- Email *Electronic Mail Service (SMTP/POP3-IMAP4)*
- HTTP Proxy *HTTP Proxy Service*
- Shared files *File sharing and authentication service*
- IDS *Intrusion Detection System (IDS)*

You can also receive notifications of the following events:

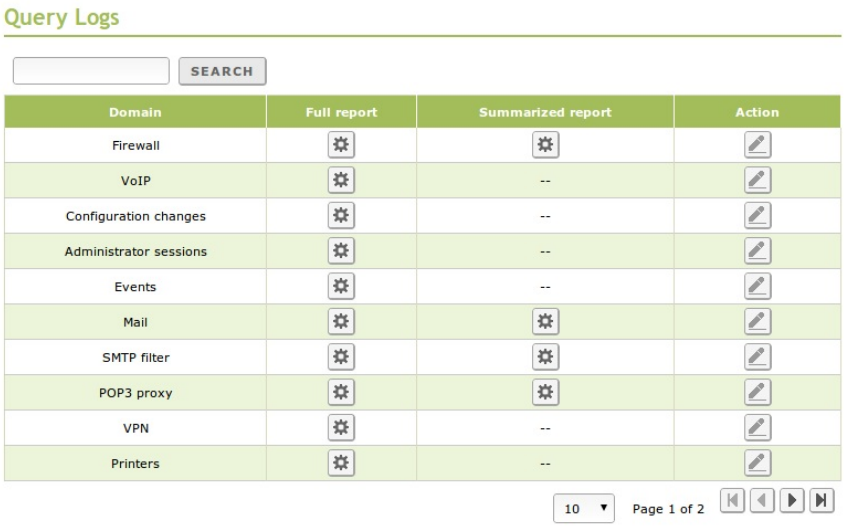
- Specific values in the logs.
- Zentyal health status.
- Service status.

- Events of the RAID subsystem per *software*.
- Free disk space.
- Problems with the outgoing *Internet routers*.
- Completion of a full data backup.

To start with, to be able to work with the **logs**, just like with any other Zentyal module, you must make sure that the module has been enabled.

To enable the module, go to *Module status* and check the *logs* box. To obtain reports from the existing logs, you can go to the *Maintenance* ▸ *Logs* ▸ *Query logs* section via the Zentyal menu.

You can obtain a *Full report* of all log domains. Moreover, some of them provide an interesting *Summarised Report*; giving you an overview of the service during a time period.



Query log screen

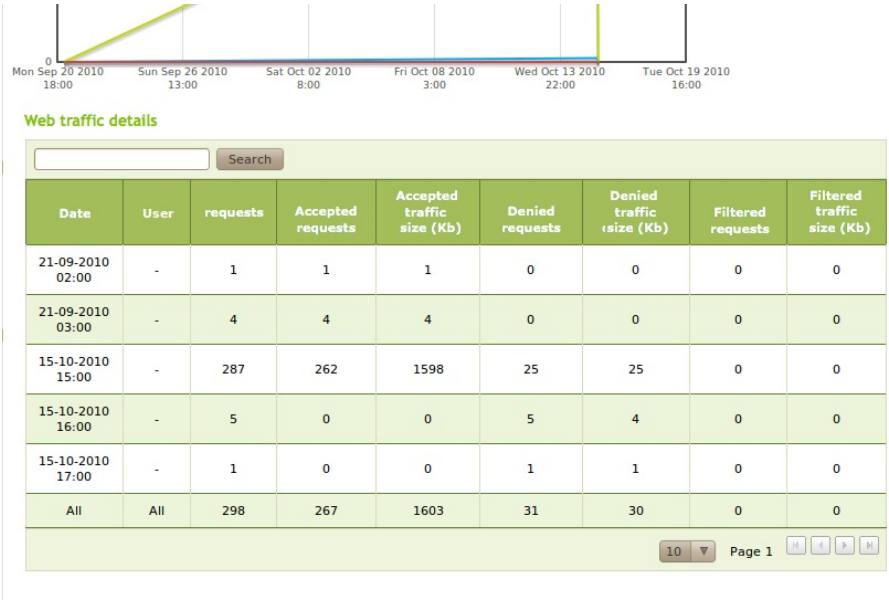
In the *Full report* you have a list of all registered actions for the selected domain. The information provided depends on each domain. For example, for the *OpenVPN* domain you can see the connections to a VPN server of a client with a specific certificate or for example, for the *HTTP Proxy* you can see the pages denied to a specific client. Therefore, you can create a customised query which allows you to filter by time period or other values that depend on the type of domain. You can store these queries as events so that you will be notified when a match occurs. Furthermore, if the query doesn't have an upper time

limit, the results will automatically refresh with new data.

Date	Input interface	Output interface	Source	Destination	Protocol	Source port	Destination port	Decision
2012-09-22 18:57:56	eth1		192.168.56.1	192.168.56.252	TCP	51790	443	LOG
2012-09-22 18:57:55	eth1		192.168.56.1	192.168.56.252	TCP	51787	443	LOG
2012-09-22 18:57:54	eth1		192.168.56.1	192.168.56.252	TCP	51787	443	LOG
2012-09-22 18:57:54	eth1		192.168.56.1	192.168.56.252	TCP	51787	443	DROP
2012-09-22 18:57:54	eth1		192.168.56.1	192.168.56.252	TCP	51788	443	LOG
2012-09-22 18:57:54	eth1		192.168.56.1	192.168.56.252	TCP	51789	443	LOG
2012-09-22 18:57:53	eth0		192.168.1.131	255.255.255.255	UDP	17500	17500	DROP
2012-09-22 18:57:53	eth0		192.168.1.131	192.168.1.255	UDP	17500	17500	DROP

Full report screen

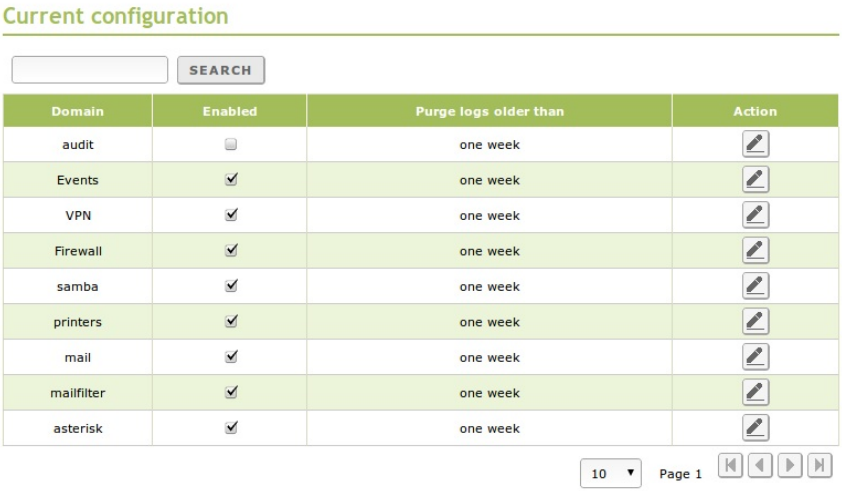
The *Summarised reports* allow you to select the time period of the report, which may be one hour, one day, a week or a month. The information you obtain is one or more graphics, together with a summary table with total values of different data types. In the image you can see, for example, daily request statistics and daily *HTTP Proxy* traffic.


0
Mon Sep 20 2010 18:00
Sun Sep 26 2010 13:00
Sat Oct 02 2010 8:00
Fri Oct 08 2010 3:00
Wed Oct 13 2010 22:00
Tue Oct 19 2010 16:00
Web traffic details
Search
Date
User
requests
Accepted requests
Accepted traffic size (Kb)
Denied requests
Denied traffic size (Kb)
Filtered requests
Filtered traffic size (Kb)
21-09-2010 02:00 - 1 1 1 0 0 0 0
21-09-2010 03:00 - 4 4 4 0 0 0 0
15-10-2010 15:00 - 287 262 1598 25 25 0 0
15-10-2010 16:00 - 5 0 0 5 4 0 0
15-10-2010 17:00 - 1 0 0 1 1 0 0
All All 298 267 1603 31 30 0 0
10
Page 1

Summarised report screen

Configuration of Zentyal logs

Once you have seen how to check the logs, it is also important to know that you can configure them in the *Maintenance ▸ Logs ▸ Configure logs* section from Zentyal menu.



Log configuration screen

The values you can configure for each installed domain are:

Enabled:

If this option is not enabled, no logs are written for this domain.

Purge logs older than:

This option establishes the maximum time during which the logs will be saved. All the values that are older than the specified time will be discarded.

In addition, you can also force the instant removal of all the logs before a certain time period. You can do this by clicking on the *Purge* in the *Force log purge* section. This allows selection of different intervals, ranging from one hour to 90 days.

Log Audit for Zentyal administrators

In addition to the logs available for the different Zentyal services, there are two other log registries not associated with any of the services, but rather with the Zentyal's administrative panel itself. This feature is specially useful for servers managed by more that one person, since you have a stored log of the successive configuration changes, and executed actions for each user, with their associated timestamps.

By default, this feature is disabled. If you want to enable it, you just have to go to *Maintenance* ▸ *Logs* ▸ *Configure logs* and enable the *audit* domain, as explained in the former section.

Setting up audit log

Once you have saved these changes, go to *Maintenance* ▸ *Logs* ▸ *Query logs* to see the following two tables:

- Configuration changes: Here you can see the module, section, type of event, and current and former changes (if applicable) for all the configuration changes made after the audit log was enabled.
- Administrator sessions: It contains the information related with all the administration login attempts, successful or not, session log outs and expired sessions for the different users, with their associated IP addresses.

Date/Time	User	IP	Event
2012-09-22 19:10:04	administrator	192.168.56.1	Login
2012-09-22 19:10:02	administrator	192.168.56.1	Logout

Query administration logs

Since there are some actions in Zentyal that take effect instantly, like restarting a server, and some others that are not applied until you save the changes, like most of the configuration changes, the audit log treats them in a different way. The instant actions will be logged permanently (until the registry is purged) and the ones pending to save will be displayed in the save changes interface itself, offering the system administrator a summary of all the modifications since the last save point, or, in case you want to discard changes, the actions will be removed from the log.

Logs saving changes

Copyright 2004-2012 Zentyal S.L.

Events and alerts

Events and alerts configuration in Zentyal

The **events** module is a convenient service that allows you to receive notifications of certain events and alerts that occur on your Zentyal server.

Zentyal allows you to receive these alerts and events via the following dispatchers:

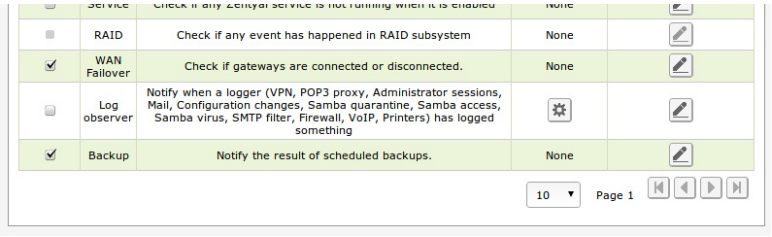
- Mail [1]
- Jabber
- Logs
- RSS

[1] The **mail** module needs to be installed and configured. (*Electronic Mail Service (SMTP/POP3-IMAP4)*).

Before enabling any event you have to make sure that the events module is enabled. Go to *Module status* and check the *events* module.

Unlike the Logs module, where all services are enabled by default except the **firewall**, you need to enable the events that might be of interest to you.

To enable an event, you have to click on the menu entry *Maintenance* ▸ *Events* ▸ *Configure Events* and mark the *Enabled* box.



	Service	Check if any Zentyal service is not running when it is enabled	None	
	RAID	Check if any event has happened in RAID subsystem	None	
☑	WAN Failover	Check if gateways are connected or disconnected.	None	
	Log observer	Notify when a logger (VPN, POP3 proxy, Administrator sessions, Mail, Configuration changes, Samba quarantine, Samba access, Samba virus, SMTP filter, Firewall, VoIP, Printers) has logged something		
☑	Backup	Notify the result of scheduled backups.	None	

10 Page 1

Configure events page

There are some events that need further configuration to work properly. This is true for the log and free storage space monitoring.

The configuration of the free storage monitoring is straightforward. The only required parameter is the free space percentage value that will trigger the event as it occurs.

For the log monitor, first you need to select which domains you want to use to generate events. For every domain, you can add filtering rules that depend on the domain. Some examples are: denied HTTP requests by the proxy, DHCP leases for a given IP, cancelled printer jobs, and so on. You can also create an event filter from an existing log query by clicking on the *Save as an event button* through *Maintenance* ▸ *Logs* ▸ *Query Logs* ▸ *Full Report*.

To control the selection of channels for event notification, select the event dispatchers in the *Configure dispatchers* tab.

SEARCH

Enabled	Name	Receiver	Configuration	Action
	RSS	RSS file: Alerts		
	Zentyal Remote	Zentyal Remote		
✓	Log	Log file	None	
	Jabber	Jabber Account		
	Mail	Mail Account		

10 Page 1

Configure dispatchers page

In a similar way, to enable events, you need to mark the *Enabled* box. Except for the log watcher, which writes its output to */var/log/zentyal/zentyal.log*, all the other dispatchers require more configuration:

Mail:

You need to set the recipient's email address (usually the Zentyal

administrator). You can also set the subject of the messages.

Jabber:

You need to set the Jabber server address and port that will be used to send the messages. You also need to set the username and password of the user that will send the messages and the Jabber address of the administrator who will receive the notifications. From this page you can also create a new Jabber account with these new parameters in case they do not exist.

RSS:

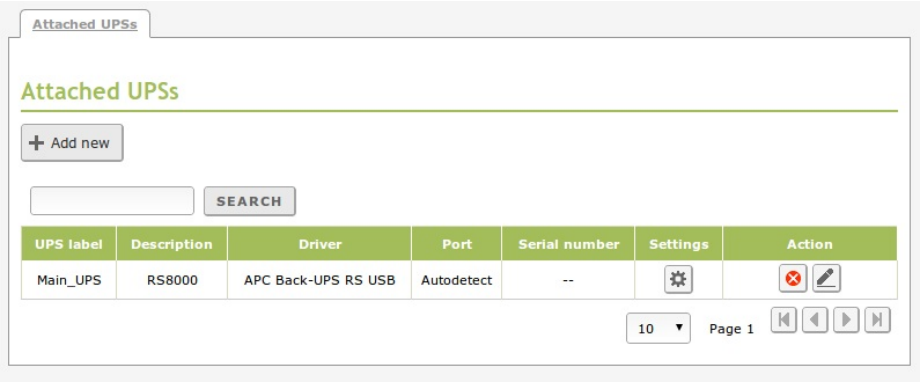
You can select the policy for authorised readers, as well as the feed link. The public feed can be made private or authorised by source IP, address or object.

Copyright 2004-2012 Zentyal S.L.

Uninterruptible power supply

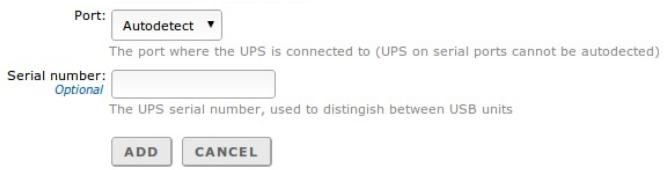
UPS Configuration with Zentyal

If you want to configure an UPS with Zentyal, you will have to connect it to your server. Install and enable the *UPS Management* module and go to *Maintenance ▸ UPS*



List of configured UPS

You have to fill the following parameters to configure a new UPS hardware.


Port:
Autodetect
The port where the UPS is connected to (UPS on serial ports cannot be autodected)
Serial number:
Optional
The UPS serial number, used to distingish between USB units
ADD
CANCEL

Adding a new UPS

UPS label

Label to name this UPS.

Description

Description associated to this UPS.

Driver

Driver that will manage the data read and write in our UPS, you have to enter the manufacturer in the left field and model in the next one. In the last field you can see the associated driver.

Port

UPS using serial ports can not be auto detected, so you will need to specify the port. If you are using USB UPS *Autodetect* should be enough.

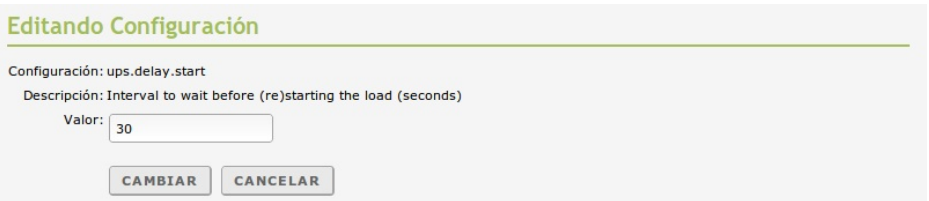
Serial number

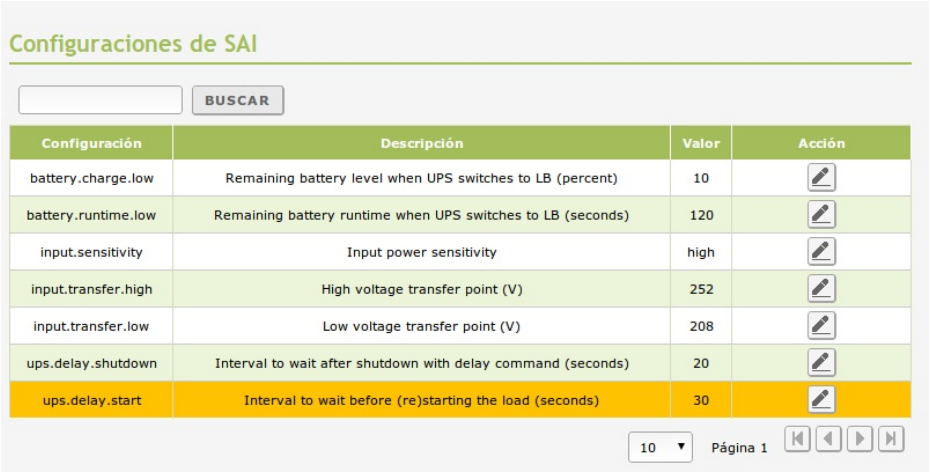
In case you have several UPS attached to your server's USB, you can stablish specific configuration differentiated by the serial number.

If you go to *Configuration* of your UPS, you can edit the configurations and browse the avaiable variables.

Warning: Depending on the model of your UPS, different configuration parameters will be published. However, they usually have a similar set of parameters and names.

Example of available configurations for our UPS:

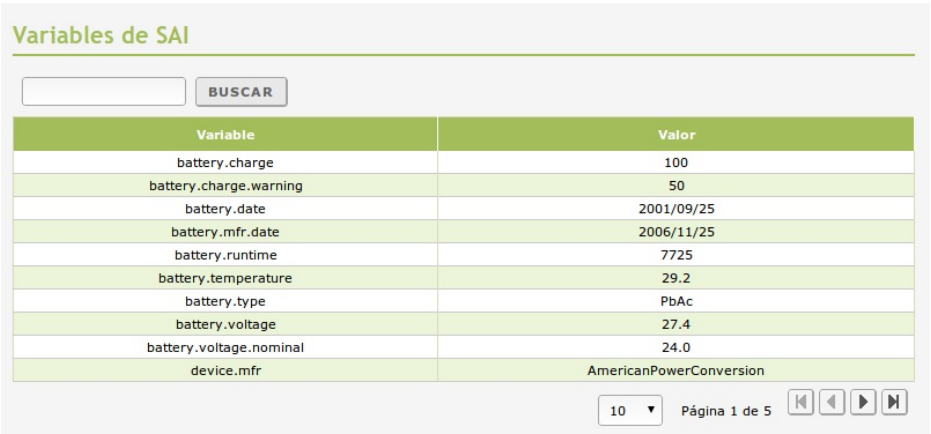




Available configuration parameters

If you go to *UPS settings* you will see a list of modifiable parameters. Some of the most used will be *ups.delay.shutdown (Time delay after sending the shutdown signal to the server when the UPS shuts down itself) or *battery.charge.low* (battery threshold to send the shutdown signal to the server).

Example of variables available for the UPS



UPS Variables

The *variables* are read-only parameters for example *battery.charge* or *battery.temperature*

Copyright 2004-2012 Zentyal S.L.

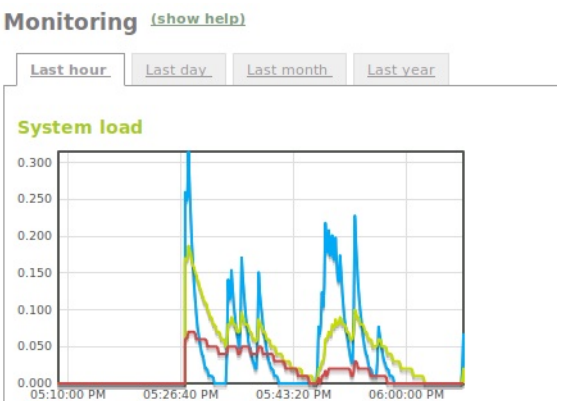
Monitoring

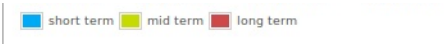
Monitoring in Zentyal

The **monitor** module allows the administrator to view the status of system resources from the Zentyal server. This information is essential to assist with both troubleshooting and advanced planning of resources in order to avoid problems.

Monitoring is displayed using graphics which give a quick overview of resource usage trends. You can see the graphical monitor by viewing the menuselection:*Monitor* module. Placing the cursor somewhere over the line on the graphic you are interested in, the exact value for a given instant can be determined.

You can choose the time scale of the graphics to view an hour, a day, month or year. To do this, simply click on the tab you are interested in.



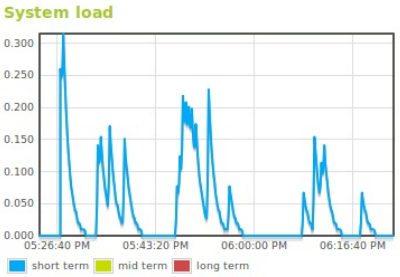


Tabs with the different monitoring reports

Metrics

System load

The **system load** attempts to measure the rate of pending work over the completed work. This metric is defined as the number of runnable tasks in the run-queue and is provided by many operating systems as a one, five or fifteen minutes average.

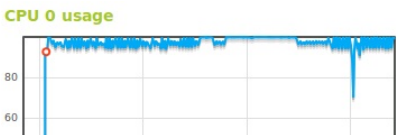


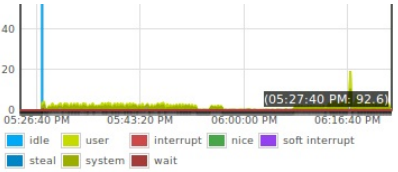
System load graphic

CPU usage

This graphic shows detailed information of the **CPU usage**. For multi-core or multi-cpu machines you will see one graphic for each core.

These graphics represent the amount of time that the CPU spends in each of its states: running user code, system code, inactive, input/output wait, and so on. The time is not a percentage, but scheduling units known as *jiffies*. In most *Linux* systems this value is 100 per second, but this may differ.





CPU usage graphic

Memory usage

This graphic displays the **memory usage**. The following variables are monitored:

Free memory:

Amount of memory not used

Page cache:

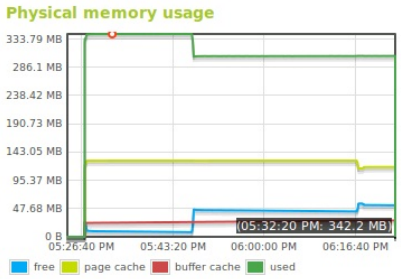
Amount of memory that is cached in a disk swap

Buffer cache:

Amount of memory that is cached for input/output operations

Memory used:

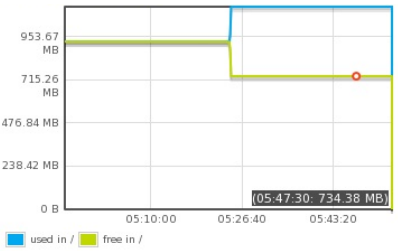
Amount of memory that is not included in any of the above



Memory usage graphic

File system usage

This graphic displays the used and free space of every mount point.

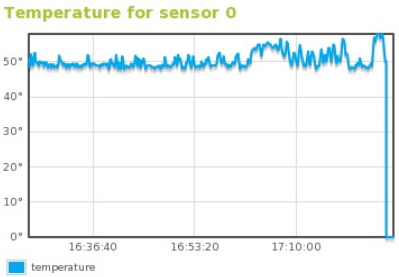


File system usage graphic

Temperature

This graphic allows you to view the system temperature in Celsius degrees by using the ACPI system [1]. In order to enable this metric, the server must have this system installed and the kernel must support it.

[1] *Advanced Configuration and Power Interface* (ACPI) is an open standard to configure devices focused on operating systems and power management. http://www.acpi.info/



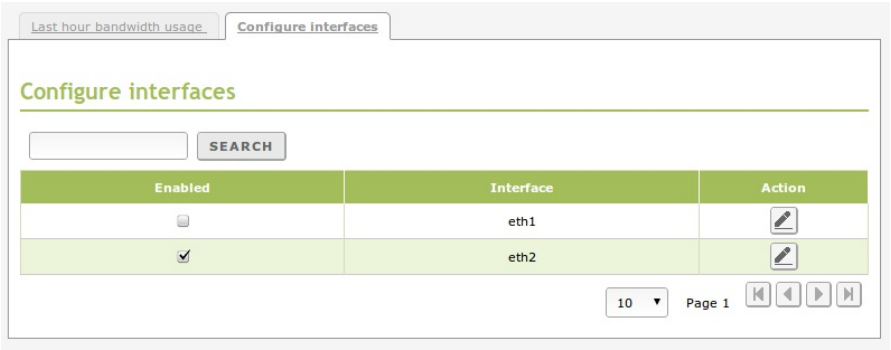
Temperature sensor diagram graphic

Bandwidth Monitoring

Besides the monitoring module, there is also a **Bandwidth Monitoring** module, which monitors the network flow. Using this module you can study the network use for each client connected to Zentyal's internal networks.

Once you have installed and enabled the module, you can access it

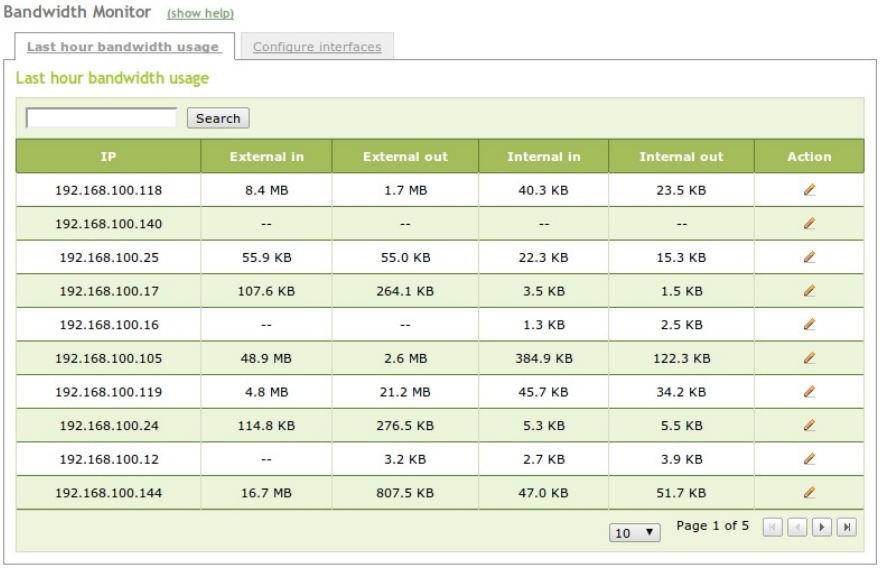
through *Network –> Bandwidth Monitor*.



Configuration tabs for the interfaces to monitor

Configure interfaces

In this tab you can configure the internal interfaces you are going to monitor. By default it is enabled for all of them.


Bandwidth Monitor
(show help)
Last hour bandwidth usage
Configure interfaces
Last hour bandwidth usage
Search
IP
External in
External out
Internal in
Internal out
Action
192.168.100.118 8.4 MB 1.7 MB 40.3 KB 23.5 KB
192.168.100.140 -- -- -- --
192.168.100.25 55.9 KB 55.0 KB 22.3 KB 15.3 KB
192.168.100.17 107.6 KB 264.1 KB 3.5 KB 1.5 KB
192.168.100.16 -- -- 1.3 KB 2.5 KB
192.168.100.105 48.9 MB 2.6 MB 384.9 KB 122.3 KB
192.168.100.119 4.8 MB 21.2 MB 45.7 KB 34.2 KB
192.168.100.24 114.8 KB 276.5 KB 5.3 KB 5.5 KB
192.168.100.12 -- 3.2 KB 2.7 KB 3.9 KB
192.168.100.144 16.7 MB 807.5 KB 47.0 KB 51.7 KB
10
Page 1 of 5

Tab detailing the badwidth usage in the last hour

Last hour bandwidth usage

Here you can see a list of the bandwidth usage during the last

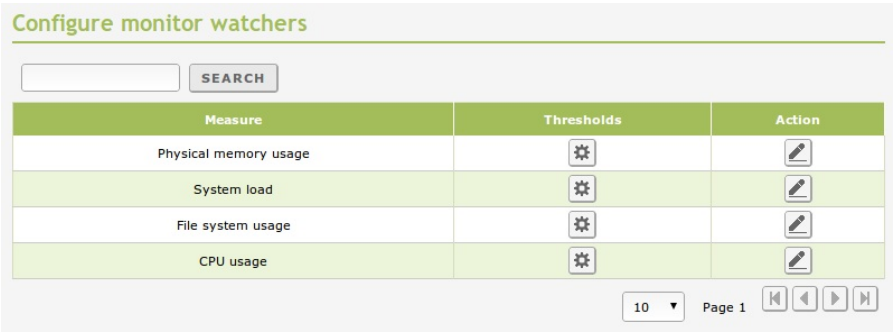
hour for all the clients connected to the monitored interfaces. The columns show, for each client IP, the amount of traffic trasmitted to and from the external network and the internal networks.

Warning: The data in this tab is updated every 10 minutes, thus, you will not have any available information for the first moments after configuring and enabling the module.

Alerts

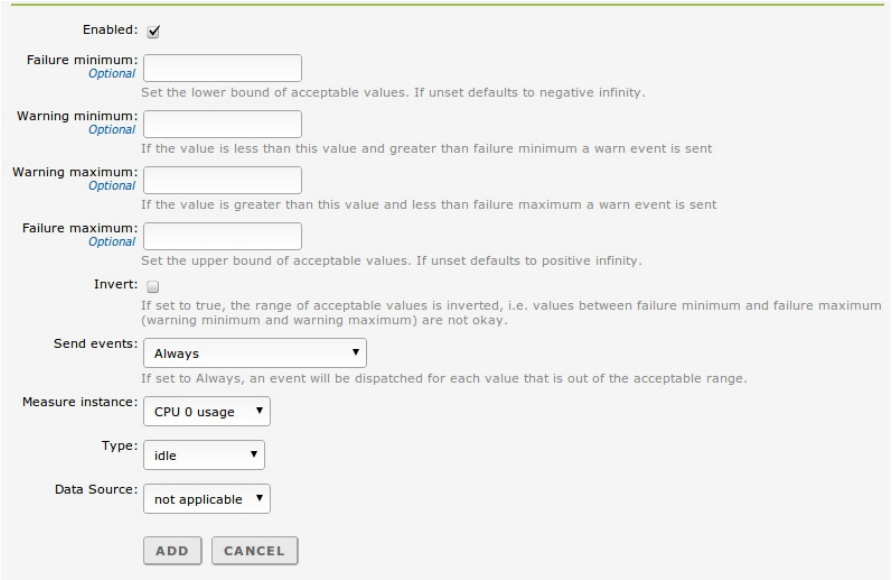
The monitoring system would be largely unused if it was not coupled with a notification system to warn users when uncommon values are produced. This ensures that you know when the host is suffering from an unusual load or is close to maximum capacity.

Monitoring alerts are configured in Events module. Go to *Maintenance* ▸ *Events* ▸ *Configure Events*; here you can see the full list of available alerts, the relevant events are grouped in the *Monitor* event.



Configuration screen for the monitor observers

Clicking on the cell configuration, you access the event configuration. You can choose any of the monitored metrics and establish thresholds which trigger events.


Enabled:
Failure minimum:
Optional
Set the lower bound of acceptable values. If unset defaults to negative infinity.
Warning minimum:
Optional
If the value is less than this value and greater than failure minimum a warn event is sent
Warning maximum:
Optional
If the value is greater than this value and less than failure maximum a warn event is sent
Failure maximum:
Optional
Set the upper bound of acceptable values. If unset defaults to positive infinity.
Invert:
If set to true, the range of acceptable values is inverted, i.e. values between failure minimum and failure maximum (warning minimum and warning maximum) are not okay.
Send events:
Always
If set to Always, an event will be dispatched for each value that is out of the acceptable range.
Measure instance:
CPU 0 usage
Type:
idle
Data Source:
not applicable
ADD
CANCEL

Configuration screen for event thresholds

There are two different thresholds, *warning* and *failure*, this allows the user to filter events based on severity. You can use the option *reverse:* to swap the values that are considered right and wrong. Other important option is *persistent:*. Depending on the metric you can also set other parameters, for instance, you can receive alerts for the free space in hard disk metric, or the short term load in system load metric and so on.

Each measure has a metric that is described as follows:

System load:

The values must be set in **average number of runnable tasks in the run-queue**.

CPU usage:

The values must be set in **jiffies** or units of scheduling.

Physical memory usage:

The values must be set in **bytes**.

File system:

The values must be set in **bytes**.

–

Temperature:

The values must be set in **degrees**.

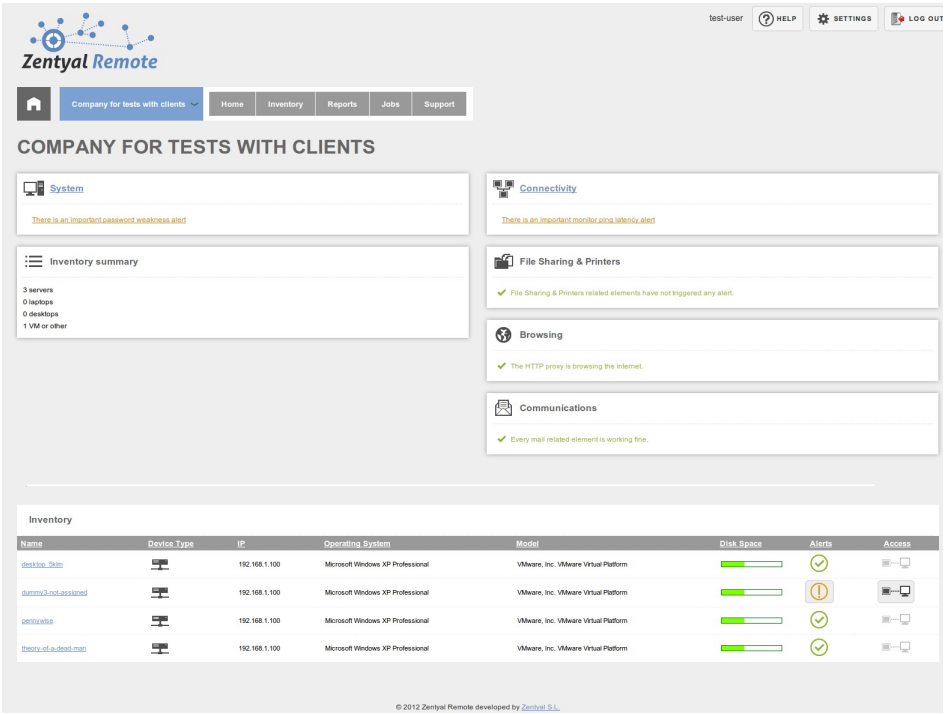
Once you have configured and enabled the event at least one observer must also be configured. The observer configuration is the same as the configuration of any other event. Check the *Events and alerts* chapter for more information.

Copyright 2004-2012 Zentyal S.L.

Automatic Maintenance with Zentyal Remote

Zentyal Remote

Zentyal Remote is a remote monitoring and management platform offered to the users of the commercial Zentyal server editions, and it is specially designed to ease the tasks of system administrators and managed service providers. This platform allows to centralize the IT infrastructure maintenance and troubleshooting of any business or a group of businesses, as well as to access remotely in a secure way to both servers and desktops.

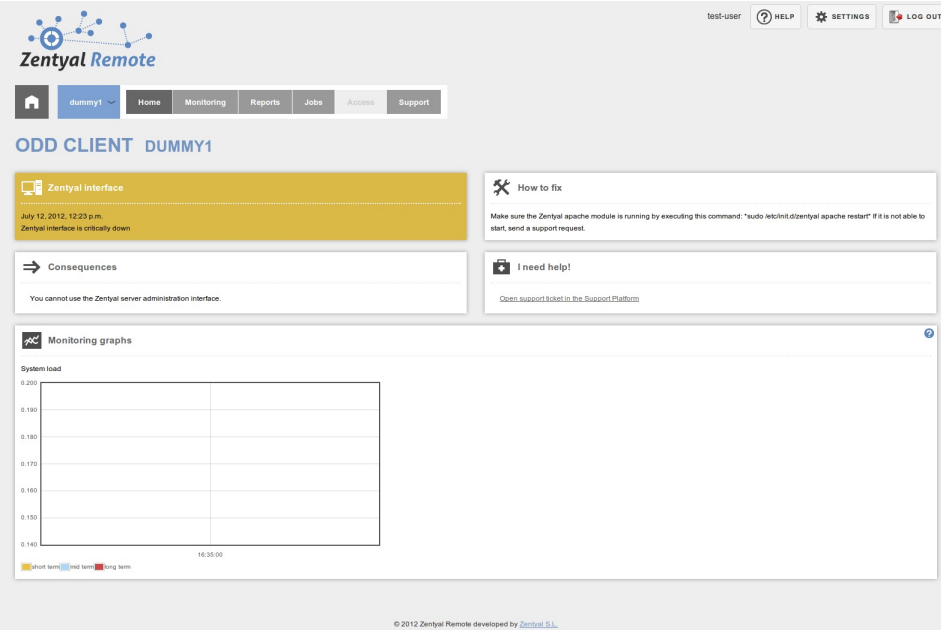


Zentyal Remote *Dashboard*

Troubleshooting

Zentyal Remote offers a quick and proactive way to identify and resolve incidents. By combining alerts, inventory information,

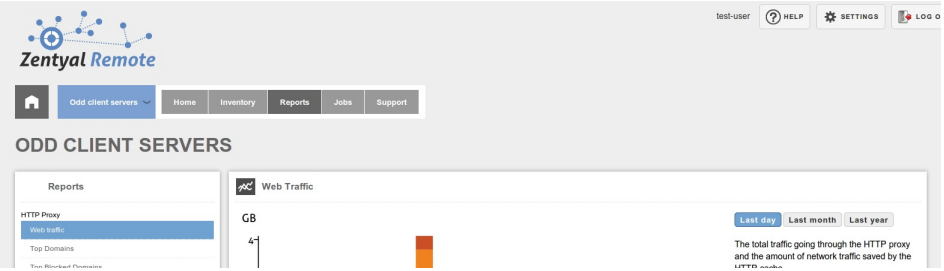
monitoring, automated diagnostics, knowledgebase, remote access and technical support, it is possible to solve issues before they affect the users' work. The concept of Zentyal Remote is similar to that of Zentyal server: different components are integrated in simple way and Linux knowledge is not required to use the tool and therefor it is easier and faster to provide remote support to multiple installations or customers simultaneously.



Problem fix

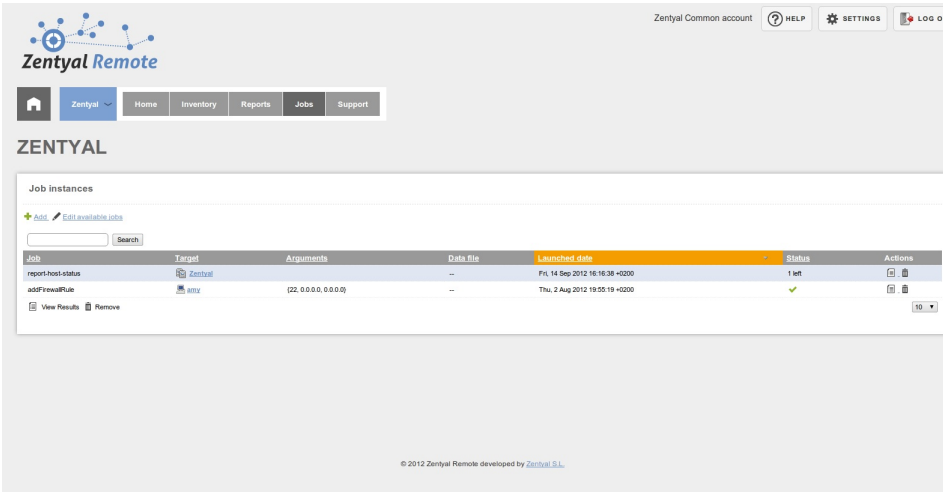
Maintenance

Zentyal Remote generates reports of the system and user activity, making it easier to maintain. For example, it is possible the determine whether a slowdown in the Internet connection is due to misconfiguration of the routers, failure of the IP provider, increased demand from the users or massive download of inappropriate content by specific users (and who they are). It is also possible to analyze the time your users spend on browsing Facebook or other similar pages and to decide whether you will apply more restrictive browsing policies to all users, by groups or to specific users only.



Server report

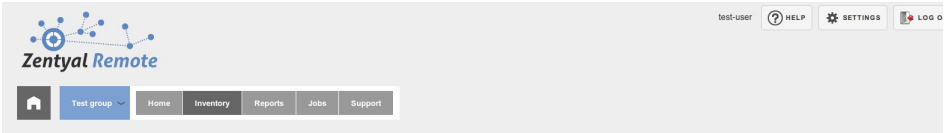
On the other hand, Zentyal Remote helps to carry out software and security updates remotely on a group of servers. Thus, one can increase the system security and at the same time reduce the maintenance costs. However, the group tasks (jobs) are not limited to updates, but can be extended to any area of the Zentyal server, from modification of firewall rules to users and groups management and to add file sharing rules. This feature is specially useful when managing a large number of servers with similar characteristics.

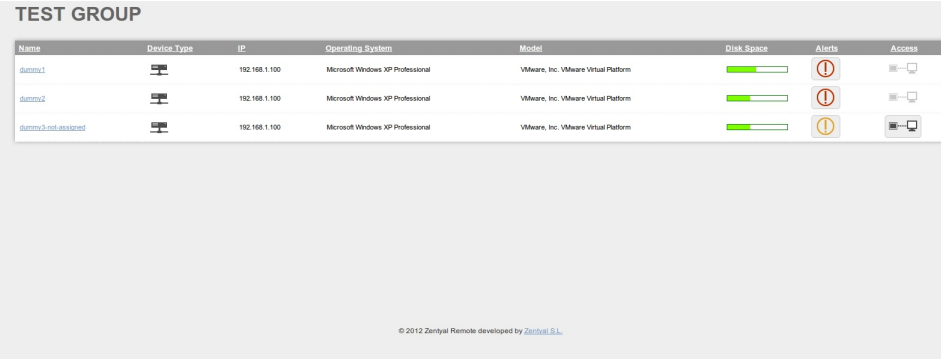


Group task management

Remote management and inventory

The possibility to remotely access servers and desktops is critical to provide remote support to end users. This remote access is carried out in a secure way through web, avoiding plenty of trips and it is the key to provide quality service at a competitive price. Moreover, the issues can be scaled to the Zentyal Support team that, with the support of Canonical, can diagnose and find solution to the reported issues. Finally, the hardware and software inventory of the equipments helps to document and manage the available network resources.





Inventory management

Free trials

Zentyal Remote is included in all the commercial Zentyal server editions. To try it, all you need to do is to get 30-day free trial through the Zentyal website [#].

[1] http://www.zentyal.com/

Copyright 2004-2012 Zentyal S.L.

Importing configuration data

Although Zentyal UI interface greatly eases the system administrator work, some configuration tasks through the interface can be tedious if you have to perform them repeatedly. For example, adding 100 new user accounts or enabling an e-mail account for all 100 users.

These tasks can be automated easily through the *Application Programming Interface* (API) which is provided by Zentyal. You only need a basic knowledge of *Perl* [1], and to know the public methods exposed by the Zentyal modules you want to use. In fact, Zentyal web interface uses the same programming interface.

[1] **Perl** is a high-level, general-purpose, interpreted, dynamic programming language. http://www.perl.org/

An example on how to create a small utility is shown below, using the Zentyal API to automatically add an arbitrary number of users defined in a *Comma Separated Values* (CSV) file

```
#!/usr/bin/perl

use strict;
use warnings;

use EBox;
use EBox::UsersAndGroups::User;

EBox::init();

my @users;
```

```
open (my $USERS, 'users');

while (my $line = <$USERS>) {
    chomp ($line);
    my $user;
    my ($username, $givenname, $surname, $password) = s
    $user->{'user'} = $username;
    $user->{'givenname'} = $givenname;
    $user->{'surname'} = $surname;
    $user->{'password'} = $password;
    push (@users, $user);
}
close ($USERS);

foreach my $user (@users) {
    EBox::UsersAndGroups::User->create($user, 0);
}

1;
```

Save the file with the name *bulkusers* and grant it execution permission using the following command: `chmod +x bulkusers`.

Before running the *script*, you must have a file called *users* in the same directory. The appearance of this file should be as follows:

```
jfoo,John,Foo,jfoopassword,
jbar,Jack,Bar,jbarpassword,
```

Finally, you must be in the directory where the files are placed and run:

```
sudo ./bulkusers
```

This section has shown a small example of task automation using the Zentyal API, but the possibilities are almost unlimited.

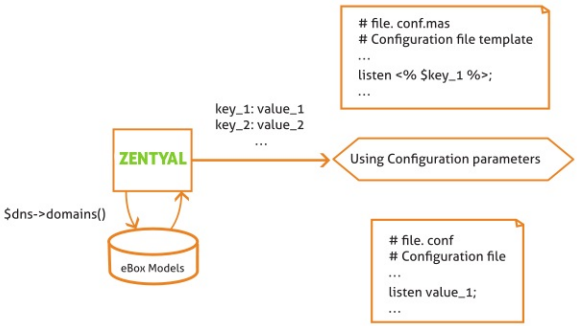
Advanced Service Customisation

This section discusses two options for system customisation for users with special requirements:

- Tailor service configuration files managed by Zentyal.
- Perform actions in the process of saving changes in configuration.

When a module is responsible for automatically setting up a service, it tries to cover the most common configuration options. However, there are cases where there are so many configuration settings that it would be impossible for Zentyal to control them all. In addition to this, one of the main goals of Zentyal is simplicity. However, there are users who want to adjust some of those unhandled parameters to adapt Zentyal to their requirements. One of the possibilities of doing this is by editing the configuration files that handle the service directly.

Before deciding to modify a configuration file manually, you must understand how Zentyal works internally. The Zentyal modules, once enabled,overwrite the original system configuration files for the services they manage. Modules do this through **templates** that essentially contain the basic structure of a typical configuration file for the service. However, some of the parts are parametrised through variables. The values of these variables are assigned before overwriting the file and are taken from the configuration previously set using the Zentyal web interface.



How the configuration template system works

Therefore, if you want to make your changes persistent, and prevent them from being overwritten every time Zentyal saves changes, you must edit templates instead of system configuration files. These templates are in */usr/share/zentyal/stubs* and their names are the original configuration file names plus the *.mas* extension.

Take into account that these changes will persist even if you modify the Zentyal configuration; they will not apply anymore if you update the module containing the template. When you reinstall a package the *.mas* files will be overwritten. If you want these changes to be effective even when you update the module, you have to copy the template to `/etc/zentyal/stubs/` inside the directory with the name of the module. This way, if you want, for example, to modify the template:file:*/usr/share/zentyal/stubs/dns/named.conf.options.mas*, you will create the directory `/etc/zentyal/stubs/dns/`, copy the template inside and modify this copy:

```
sudo mkdir /etc/zentyal/stubs/dns
sudo cp /usr/share/zentyal/stubs/dns/named.conf.options
```

Another advantage of copying the templates to `/etc/zentyal/stubs/` is that you can keep control of the modifications that you have done over the original templates, and you will always be able to check these differences using the 'diff' tool. For example, for the former case:

```
diff /etc/zentyal/stubs/dns/named.conf.options.mas /usr
```

It is possible that you need to perform certain additional actions while Zentyal is saving changes instead of customising configuration files. For example, when Zentyal saves changes related to the firewall, the first thing the firewall module does is to remove all existing rules, and then add the ones configured in Zentyal. If you manually add a custom **iptables** rule that is not covered by Zentyal interface, it will disappear when saving firewall module changes. To prevent that, Zentyal lets you run *scripts* while the saving changes process is being performed. There are six points during the process when you may execute these *scripts*, also known as *hooks*. Two of them are general and the remaining four are per module:

Before saving changes:

- In */etc/zentyal/pre-save* directory all *scripts* with running permissions are run before starting the save changes process

permissions are run before starting the save changes process.

After saving changes:

Scripts with running permissions in */etc/zentyal/post-save* directory are executed when the process is finished.

Before saving module configuration:

Writing */etc/zentyal/hooks/<module>.presetconf* file being <*module*> the module name you want to tailor, the hook is executed prior to overwriting the module configuration. It is the ideal time to modify configuration templates from a module.

After saving module configuration:

/etc/zentyal/hooks/<module>.postsetconf file is executed after saving <*module*> configuration.

Before restarting the service:

/etc/zentyal/hooks/<module>.preservice is executed. This script could be useful to load Apache modules, for instance.

After restarting the service:

/etc/zentyal/hooks/<module>.postservice is executed. In the **firewall** case, all the extra rules must be added here.

These options have great potential and allow highly customisable Zentyal operations, offering better integration with the rest of the systems.

Development environment of new modules

Zentyal is designed with extensibility in mind and it is relatively simple to create new Zentyal modules.

Anyone with *Perl* language knowledge may take advantage of the Zentyal development framework to create web interfaces, and also benefit from the integration with the rest of the modules and the common features from the vast Zentyal library.

Zentyal design is completely object-oriented and it takes advantage of the Model-View-Controller (MVC) design pattern [2], so the developer only needs to define those features required by the data model. The remaining parts are generated automatically by Zentyal. To simplify the process further, a development tool called **zmoddev** [3] is provided to ease the development of new modules, auto-generating templates depending on the parameters provided by the user. This will save time, however, its explanation and development is beyond the scope of this course.

[2] An explanation about Model-View-Controller design pattern http://en.wikipedia.org/wiki/Model_View_Controller.

[3] **zmoddev** SVN repository access svn://svn.zentyal.org/zentyal/trunk/extra/zmoddev.

Zentyal is designed to be installed on a dedicated machine. This recommendation is also extended to the developing scheme. Developing on the same host is highly discouraged. The recommended option is to deploy a virtual system to develop as *Appendix A: Test environment with VirtualBox* explains in depth.

Release policy

Zentyal server development follows time based release cycle: a stable Zentyal release is published once a year, in September. The Zentyal Development Team has opted for time based release cycle most importantly because it makes easier, for both users and for developers, to make long-term decisions regarding the development, deployment and maintenance of the server and helps the Development Team to deliver well tested, high-quality software.

It is important to notice that all Zentyal releases are based on the Ubuntu LTS versions. Each Zentyal release is based on the Ubuntu LTS version that is available at the moment the release is launched.

Zentyal Release Cycle

There are three types of Zentyal server releases the Zentyal Development Team will publish during the Zentyal Release Cycle: Beta versions, Release Candidates and Stable versions. The stable versions will be supported for three years after which they reach their "end of life" date and become unsupported.

Zentyal Beta versions

Zentyal Beta versions are unstable software releases that are published from September to June. These beta versions introduce new features that are not yet fully tested for bugs. As the Zentyal Development Team follows the "Release early, release often" guideline, there might be an important number of beta versions published during this time period.

Beta releases always have odd major numbers: 1.1, 1.3, 1.5, 2.1, 2.3...

As Beta versions will eventually become stable releases, this means that 2.1 series followed this pattern: 2.1.1, 2.1.2, 2.1.3, ... 2.1.10, 2.1.11, 2.1.x -> 2.2

The 2.3 series will follow this pattern: 2.3.1, 2.3.2, 2.3.3, ... 2.3.10, 2.3.11, 2.3.x -> 3.0

Zentyal Release Candidates

Zentyal Release Candidates are published from July to September, during the three months stabilization period. There are as many release candidates as the Development Team deems necessary to stabilize the new code and bug fixes introduced before publishing the next stable version.

Release candidates always have the version number of the next stable release and the "rc" suffix to indicate that the version is a release candidate. A suffix of "rc1" would be used for the first release candidate, "rc2" for the second release candidate, "rc3" for the third release candidate, and so on: 3.0-rc1, 3.0-rc2...

Stable Zentyal versions

Stable Zentyal versions are published once a year, in September. Stable releases always have even major numbers: 1.0, 1.2, 1.4, 2.0, 2.2, 3.0... The first version number changes every time the base system, Ubuntu LTS version, is upgraded.

For example, the versions 1.0, 1.2 and 1.4 were based on Ubuntu 8.04 LTS , 2.0 and 2.2 were based on Ubuntu 10.04 LTS and the 3.0 will be based on Ubuntu 12.04 LTS.

Timetable

- June: Zentyal development is frozen. Three months stabilization period starts. The necessary release candidate versions are published during this period.
- September: Stable Zentyal version is published.
- October-June: Zentyal development continues. The necessary beta versions are published during this period.

Support policy

The Zentyal Development Team offers three years of support for the stable Zentyal versions. This means that since the publication of a stable Zentyal version, support for all security issues as well as commercial support and subscription services will be granted for this version during the next three years. After this time period, the stable version reaches its "end of life" date and becomes unsupported.

Bug management policy

Each open source software project has its own bug management policy. As mentioned previously, the stable Zentyal versions are supported for three years during which support for all security issues is granted. In addition to security issues, other modifications might be added to fix several bugs at once. The latest Zentyal version always includes all the bug fixes.

The project management tool **Trac** [4] is used by the Zentyal

Development Team to manage bugs and other tasks. It lets users open **tickets** to report problems and it is open to all users. Once the ticket is created by a user, its state can be tracked by the user through the web or e-mail. You may reach Zentyal **Trac** at http://trac.zentyal.org.

[4] **Trac**: is an enhanced Viki and issue tracking system for software development projects http://trac.edgewall.org.

It is highly recommendable to report a bug when you are fairly sure that your problem is really a bug and not just an expected result of the program under determined circumstances.

To report a bug, check first in the **Trac** if the bug was reported already. If not, report the bug via the Zentyal web interface (if the crash appears there) or manually via the Zentyal bug tracker. If the bug was reported already, you can still help by confirming that you have reproduced it and giving additional details about the issue.

It is absolutely necessary to include detailed steps to reproduce the issue so that the Zentyal Development Team can fix it. If you are reporting manually, include at least the /var/log/zentyal/zentyal.log file or any other useful information you think it's related with your issue. Screenshots are also welcome if you think they will help to see the problem.

Finally, it is even better if you can provide a solution to the issue. This could be done by modifying the application itself through a *patch* or by following some steps to avoid the problem temporarily (*workaround*).

Patches and security updates

A **patch** is a modification in the source code used to fix a bug or add a new feature to that software. In open source projects, community members are able to send patches to the project maintainers and if the patches are considered suitable, then they will be merged into the application.

Developers themselves often publish official patches too, for example, fixing a known vulnerability. But, typically, projects like Zentyal, release a new version of the package - including the official patch.

You can check out the available community updates and install them using the web interface through the **software** module [5]. If you have a commercial server subscription [6], quality assured software updates will be automatically applied to your Zentyal server to guarantee your installation with maximum security and uptime.

[5] *Software updates* section shows this module in depth.
[6] http://www.zentyal.com/services/subscriptions/

Technical support

Open source software projects usually provide technical support to the users through different methods. Zentyal is not an exception.

You must distinguish between two kinds of support: the support provided to and by the community, which is free, and the commercial support, provided by companies that charge a fee for their services.

Community support

Community support is provided mainly on the Internet. There are many occasions in which the community is able to support itself. That is, the users help each other.

The community members are an important, even fundamental, providers of information for the product development. Users contribute by discovering hidden bugs and help developers to improve the product so it becomes more attractive to more users.

This voluntary support, logically, does not offer any guarantees. If a user asks a question, it is possible that no reply is given depending on the question format, timing or any other circumstances.

Zentyal community support channels is centered on the forum [7],

although mailing lists [8] and IRC channels [9] are also available.

[7] http://forum.zentyal.org
[8] http://lists.zentyal.org
[9] **irc.freenode.net** server, **#Zentyal** (English) and **#Zentyal-es** (Spanish) channels.

All this information is available, with further documentation, in the community section of Zentyal web site (http://www.zentyal.org).

Commercial support

The **commercial support** allows the user access to obtain support as a professional service. Unlike community support, the commercial support offered by Zentyal Development Team or Authorized Zentyal Partners offers several guarantees:

- Maximum response time: depending on the **service package** the response time will be different.
- Support from well-trained professionals backed by the Zentyal Development Team.
- Additional features which add value to the product and are not available to the community.

In addition to this, commercial support ensures no time is wasted trying to find out what hardware you should purchase, what modules you should install, how to make the initial configuration, how to integrate Zentyal with existing systems, etc. These advantages are pretty clear for companies whose business relies on this software.

Copyright 2004-2012 Zentyal S.L.